NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEVELOPING A FLY-AWAY-KIT (FLAK) TO SUPPORT HASTILY FORMED NETWORKS (HFN) FOR HUMANITARIAN ASSISTANCE AND DISASTER RELIEF (HA/DR)

by

David D. Lancaster

June 2005

Co-Advisors:	Alex Bordetsky
	Brian Steckler
Second Readers:	Rex Buddenberg
	Brian Fila

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Developing a FLy-Away-Kit (FLAK) to Support Hastily Formed Networks (HFN) for Humanitarian Assistance and Disaster Relief (HA/DR)			**5. FUNDING NUMBERS**
6. AUTHOR(S) David D. Lancaster			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This research discusses developing a FLy-Away-Kit (FLAK) to support the forming of Hastily Formed Networks (HFNs) in remote areas in support of Humanitarian Assistance and Disaster Relief (HA/DR) operations. The initial focus will be on the requirements, situation, area of operations and mission. Different definitions and perspectives emerge when an individual mentions HFNs, HA/DR and Complex Humanitarian Disasters (CHDs). It is the author's intention to define and describe both a HFN and a CHD, in order to justify the need for the FLAK. This process will also define the requirements for the FLAK as well as facilitate processes for ensuring those requirements are met.

The personnel responding to the attacks of September 11, 2001 and the December 26, 2004 Southeast Asia Tsunami suffered Command and Control (C2) and information challenges. Even more challenges are being currently addressed by Homeland Defense, Maritime Domain Awareness, and Non-Governmental Organizations (NGOs) abroad. From the top down, levels of administration are developing new plans, procedures, and organizations that will improve the security and communication processes of our nation. A global, broadband, rapidly deployable network node complete with Internet reach-back, voice, data, and video capability is of the utmost importance to enable C2 and Network Centric Operations (NCO). Undoubtedly, commercial and military organizations, traditional or new, will greatly benefit from this capability. The U.S. DoD is particularly interested in improving interaction, coordination, communications, and operations when DoD and other entities respond simultaneously to natural or man-made CHD's.

14. SUBJECT TERMS Hastily Formed Networks, HFN, Rapid deployable networking, Mobile Command Center, Ka, L Band, VSAT, 802.16, OFDM, 802.11, MESH, VoIP, C2PC			**15. NUMBER OF PAGES** 89
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

DEVELOPING A FLY-AWAY-KIT (FLAK) TO SUPPORT HASTILY FORMED NETWORKS (HFN) FOR HUMANITARIAN ASSISTANCE AND DISASTER RELIEF (HA/DR)

David D. Lancaster
Captain, United States Marine Corps
B.S., North Carolina State University, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
June 2005

Author: David D. Lancaster

Approved by: Alex Bordetsky, Thesis Co-Advisor

Brian Steckler, Thesis Co-Advisor

Rex Buddenberg, Second Reader

Brian Fila, Second Reader

Dan Boger, Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research discusses developing a FLy-Away-Kit (FLAK) to support the forming of Hastily Formed Networks (HFNs) in remote areas in support of Humanitarian Assistance and Disaster Relief (HA/DR) operations. The initial focus will be on the requirements, situation, area of operations and mission. Different definitions and perspectives emerge when an individual mentions HFNs, HA/DR and Complex Humanitarian Disasters (CHDs). It is the author's intention to define and describe both a HFN and a CHD, in order to justify the need for the FLAK. This process will also define the requirements for the FLAK as well as facilitate processes for ensuring those requirements are met.

The personnel responding to the attacks of September 11, 2001 and the December 26, 2004 Southeast Asia Tsunami suffered Command and Control (C2) and information challenges. Even more challenges are being currently addressed by Homeland Defense, Maritime Domain Awareness, and Non-Governmental Organizations (NGOs) abroad. From the top down, levels of administration are developing new plans, procedures, and organizations that will improve the security and communication processes of our nation. A global, broadband, rapidly deployable network node complete with Internet reach-back, voice, data, and video capability is of the utmost importance to enable C2 and Network Centric Operations (NCO). Undoubtedly, commercial and military organizations, traditional or new, will greatly benefit from this capability. The U.S. DoD is particularly interested in improving interaction, coordination, communications, and operations when DoD and other entities respond simultaneously to natural or man-made CHD's.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would first like to thank God for His Son who is our savior, redeemer and friend. Thank you Father for the tremendous changes you have brought about in my life. I will never forget the time spent here in Monterey. I will never forget all of the wonderful people that you have placed in my life. I promise to do my best to share with others all that you have done for me.

Next, thanks to the professors from the Naval Postgraduate School that supported this thesis with training, equipment, research, and mentorship. Dr. Alex Bordetsky, Brian Steckler, Rex Buddenberg and Eugene Bourakov all provided support and advice during the author's time at NPS. Thank you and keep up the good work. Also, thanks to Mike Clement for his valuable input and friendship.

Last, but most important I would like to thank my family for loving me through this experience. Katelyn, you are a wonderful daughter and more than I deserve. I am so proud of you. Thank you for being my friend. Cheryl, I hope that I can give you the opportunities that I have been so fortunate to have. Thanks for keeping the family going through my late nights, my mess, and my procrastination. You are a wonderful woman that deserves the best.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

We have entered an era marked with terrorist attacks, war, and disasters. All of these events have had a direct effect on the conduct of our nation that has not been experienced since the World Wars. Even more so, the September 11, 2001 attacks on U.S. soil emphasize the need for greater awareness, more thorough cross communication, and significant changes in our National Defense and the National Military Strategies. The communication and information requirements of Non-governmental Organizations (NGOs), International Organizations (IOs), and the Department of Defense (DoD) are rapidly changing within this environment. One aspect that has not changed is the use information is a strategic resource.

For more than a decade the U.S. military has been leveraging information as a strategic resource. Recently, this technique is evident in the importance placed on Network Centric Warfare (NCW) by the nation's leadership through different Transformation Planning Guidance. Leaders from the President down to the Lance Corporal realize that our forces are smaller and require a higher degree of mobility and sustainability. In order to remain effective, it is paramount that we continue to explore applications of technology that focus on improving our ability to operate as a joint, collaborative, flexible force.

Currently, we are in the process of cultural transformation with respect to applications of technology. This phase is dependant upon the continued efforts of people and the pursuit of new ideas. There is no NCW system that will present itself complete. We know that early transformation requires exploiting information technology to reform defense business practices and to create new combinations of capabilities, operating concepts, organizational relationships, and training regimes (United States Department of Defense [US DoD], 2003). The author believes that technological advances will only continue to benefit processes and decision making if it is in an environment that encourages experimentation of new ideas and implementations.

Workgroups, conferences, symposiums, papers, and live test-bed experiments focused on information technology and NCW concepts are channels that will bridge current abilities with the ideas of the future. Current test-bed experiments take place every quarter at the Naval Postgraduate School with the Tactical Network Topology efforts that focus on NCW (Tactical Network Topology [TNT] 05-2 Report, 2005). These experiments provide experience and are a source for developing technology solutions. The World Wide Consortium for the Grid (W2COG) also provides a perfect example of this type of environment. The W2COG presents a forum for using expertise and technology to speed transformation through immediate use of the global information grid (GIG) in its current state (World Wide Consortium for the Grid [W2COG], 2005).

This thesis research covers developing a FLy-Away-Kit (FLAK) to support the creation of Hastily Formed Networks (HFN) in remote areas in support of Complex Humanitarian Disasters (CHD). The initial discussion will be on the situation, area of operations, and mission. Different definitions and perspectives emerge when an individual mentions CFDs and HFNs. It is the author's intention to define and describe both a CHD and a HFN, in order to justify the need for the FLAK. This process will also attempt to define the requirements for the FLAK as well as facilitate processes for ensuring those requirements are met.

The personnel responding to the attacks on September 11, 2001 and the December 26, 2004 Southeast Asia Tsunami suffered Command and Control (C2) and information challenges. Even more challenges are being currently addressed by Homeland Defense, Maritime Domain Awareness, and Non-Governmental Organizations (NGOs) abroad. From the top down, levels of administration are developing new plans, procedures, and organizations that will improve the security and communication processes of our nation. The author believes that a global, broadband, rapidly deployable network node complete with Internet reach-back, voice, data, and video capability will facilitate these tasks through NCW principles. Undoubtedly, commercial and military organizations, traditional or new, will greatly benefit from this capability. The U.S. DoD is particularly interested in improving interaction, coordination, communications, and operations when DoD and other entities respond simultaneously to natural or man-made CHD's.

B. OBJECTIVES

This research introduces the environment faced by civil-military responders to CHDs. In an effort to accomplish their independent missions, various elements cobble together any and all available resources in efforts to build HFNs. The author intends to focus discussions on developing a FLy-Away-Kit (FLAK) with NCW tenants and CHDs in mind. Much of the discussion will be on current available commercial solutions and feedback on test of current implementations.

C. RESEARCH QUESTIONS

- What is the general situation for civil-military personnel responding to CHDs?
- What is an HFN?
- What are the types of reach-back solutions available for a FLAK?
- What emerging capabilities will a FLAK support?
- What are the basic application components that will support command, control communication, computer, and intelligence requirements?
- Can Virtual Local Area Networks (VLAN) improve the FLAK?

D. SCOPE

The scope of this research will include:

- A discussion of CHDs.
- A discussion of HFNs.
- A discussion of deployable communication systems.
- A discussion of reach-back connections.
- A discussion of last mile solutions.
- Analysis of the Cisco 2811 as the primary enabler of the FLAK.
- A discussion of Voice over IP (VoIP).
- A discussion of VLANs.
- Analysis of mesh enabled Local Area Networks (LANs).

E. METHODOLOGY

The methodology used to fulfill the requirements for this thesis will consist of the following:

- Review of articles, after action reports, and statistics from the Indian Ocean earthquake and tsunami of December 26, 2004 to discuss the characteristics of CHDs.
- Review of past thesis on related topics. This thesis uses two documents for background: Barge, Davis, Schwent thesis(2003, June) and Ford, Hogan, Perry thesis (2002, September).
- Definition of HFNs, to include discussion of the efforts of the Naval Post Graduate School to take HFNs to the tsunami stricken coast of Thailand.
- Analysis of reach-back connections for a deployable communications node. The primary focus will be on satellite connectivity to mobile and remote locations.
- Case study for FLAK development.
- Link study comparison between an 802.11b OLSR MANET and Motorola and ITT's Mesh Enabled Architecture (MEA).

F. THESIS ORGANIZATION

This thesis is organized as follows:

Chapter I Introduction – provides a brief description of the objectives of the thesis, the scope, organization, and methodology of study.

Chapter II Networking Requirements for CHDs – provides a discussion of CHDs and HFNs.

Chapter III General Configuration of Humanitarian Assistance/Disaster Relief (HA/DR) HFNs **–** overview of HFNs for HA/DR.

Chapter IV Satellite Reach-back Connections – provides a detailed look at the current state of very small aperture terminal satellite systems as the primary solution for reach-back. Additional discussion is on planning for other connections.

Chapter V Last Mile Connections – provides overview of using IEEE 802.16 implementations and WiMax to deliver connections to additional sites from a FLAK.

Chapter VI Concept of a FLAK – discussion and documentation of designing a deployable communication system.

Chapter VII FLAK Virtual Local Area Networks (VLANs)

Chapter VIII FLAK Voice Over Internet Protocol (VoIP) Service

Chapter IX FLAK Integration with Wireless Local Mesh Networks – 802.11b OLSR MANET verses Motorola and ITT's MEA. This chapter covers a link study of these two solutions for a mesh enabled LAN.

Chapter X Conclusion and Follow-on Research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. NETWORKING REQUIREMENTS FOR CHD

A. COMPLEX HUMANITARIAN DISASTERS

Most recently, the earthquake and tsunami in Southeast Asia provided a perfect study for applications of technology in support of a CHD. On December 26, 2004 massive tsunamis off the west coast of Indonesia's northern Sumatra Island were triggered by an undersea earthquake measuring 9.0 on the Richter scale. Within five days the estimated death toll had climbed to over 120,000 and claimed lives from over eleven countries (Center of Excellence in Disaster Management and Humanitarian Assistance [COE-DHMA], 2005). Within a period of thirty days those same figures had more than doubled. Responders included a wide array of personnel from national disaster management organizations, national government agencies, local government units, military-civil defense forces, United Nations agencies, international military and civil defense forces, international aid agencies, international NGOs, IOs, and private volunteers.

Across the board, most people will agree that the global response to this disaster was unprecedented. It is the author's belief that the greatest lesson learned is that it takes more effort than just throwing resources at the problem to get a solution. Human life is important, so response efforts must be conducted in a timely manner. Time, people, relationships, processes, and resources affecting HA/DR are the elements that make this business complex.

Colonel Medio Monti USMC was the C-6 for the Combined Support Force 536 and part of the U.S. Pacific Command's Multinational Planning and Augmentation Team (MPAT). Colonel Monti briefed that eleven out of thirty-three foreign militaries were present at the Combined Coordination Center (CCC), previously known as the Civil-Military Operations Center (CMOC) in Utapao, Thailand and stated, "Most of us had not worked with the world disaster response community before" (Monti, 2005). However, operating in this environment is not new to the U.S. military. The global war on terrorism and threat of using weapons of mass destruction (WMD) in general has forced response to events similar to natural disasters. These events happen without prior

warning, cause mass casualties, cause extensive damage to property, and have an impact on all communities.

In an article for *Marines Magazine* in 1999 General Krulak USMC described the issue of leadership in, "The Three Block War." Today's contingencies find Marines confronted by the entire spectrum of tactical challenges in the span of a few hours and within the space of three contiguous city blocks.

> The rapid diffusion of technology, the growth of a multitude of transnational factors, and the consequences of increasing globalization and economic interdependence, has coalesced to create national security challenges remarkable for their complexity (Krulak, 1999).

The military was not alone in placing high importance on response to complex emergencies. General Assembly Resolution 46/182 of the United Nations established the Inter-Agency Standing Committee Working Group (IASC-WG) in response to emergencies. In June of 2004, IASC-WG published a reference paper dealing with civil-military relationships in complex emergencies with an overall goal of enhancing the understanding of civil-military relations (Inter-Agency Standing Committee Working Group [IASC-WG], 2004). Information sharing was discussed previously as a strategic resource and a force enabler, but the humanitarian community raises many concerns regarding this issue. These concerns are noted in the IASC-WG document.

In his Unified Assistance brief for CSF-536, Colonel Monti makes reference to how information exchange is affected by reputations. Changes in doctrinal terminology, can play a role in fostering a successful reputation; for instance, using the terminology CCC instead of CMOC facilitated better collaboration by distancing the CCC from the past, negative perceptions of the CMOC. Historically, NGOs have felt excluded from activities in the CMOC while NGO and IO efforts have been used to further military ends. Establishing the CCC as a recognized entity for the multinational military and NGO community has fostered trust and more willingness for collaboration.

This idea of mistrust of the military by NGOs and IOs was also highlighted during the April 26, 2005 local demonstration to World Vision. The author, along with personnel from the Naval Postgraduate School and California State University at Monterey Bay, hosted a demonstration of technology and an introduction to the Military

Operations in Urban Terrain (MOUT) facility at Old Fort Ord. The demonstration was well received and inspired the following comment.

> Collaboration with the military in identifying relevant uses for technology is acceptable as long as the NGO's don't feel that the military is only doing this for use in situations where the US military has operations. These locations are relatively few in relation to the number of countries where most NGO's are deployed (World Vision, 2005).

Consequently, people are what make HA/DR complex. For that reason this problem must be recognized as ultimately a function of human behavior. The network "plumbing" is only an enabler for the people, processes and procedures to be accomplished. The "N" in NCW must be equally focused on the networking of individuals.

Interestingly, the needs and challenges faced in facilitating response to HA/DR resembles the tenets and principles of NCW:

- A robustly networked force improves information sharing
- Information sharing enhances the quality of information shared and situational awareness
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command
- These, in turn, dramatically increase mission effectiveness (Office of Force Transformation [OFT], 2005)

B. HASTILY FORMED NETWORKS

1. Overview

This section covers the author's view of HFNs. While it seems that the coined phrase has gathered much attention since the Indian Ocean earthquake and tsunami, the idea of HFNs is not really new. The enabling technologies that emerge in a crisis environment where everyone needs Internet connectivity has created an opportunity to define the concept. A HFN should operate in an unclassified realm to support all users, deal with multiple connection types to include mesh enabled clients, support disadvantaged users to include sensors, and support collaboration.

2. Classification

The root essence of a HFN is the need for people to be networked and share information. In order to facilitate a collaborative environment between the military and NGOs/IOs, the HFN should exist in an unclassified realm. The CHD environment discussed earlier laid out the large number of different personnel striving to deal with information flow. Reporter Bob Brewin recorded the following from Colonel Monti:

> What he lacked, Monti [Colonel, III MEF, USMC] said, was an unclassified network that could also be accessed by military personnel from Thailand, Indonesia, Australia and other countries, as well as representatives from the United Nations, other NGOs and U.S. civilian agencies, such as the U.S. Agency for International Development (USAID) (Brewin, 2005).

Even the unclassified Non-secure Internet Protocol Router Network (NIPRNET) posed problems for individuals who needed to exchange information with military personnel. If the information security problems are solved at the application layer, the network issue to becomes obsolete. Once free access is given to the network, the problem then becomes an information assurance problem. The requirements for this situation are concerned with the authenticity of information and confidential transactions (Buddenberg, 2005).

If HFNs continue to use leading edge technologies to fill gaps in existing networks and exploit new capabilities, the network will be unclassified just by virtue of the accreditation of the gear. It is possible to extend current security procedures to the HFN. However, most implementations will not have a certified security solution recognized by the appropriate agencies. The mission for all HA/DR efforts is to help people, but this does not mean that there are no security concerns. On the contrary, information assurance and security issues are just as important for successful operations.

3. Example HFN

The Naval Postgraduate School's efforts to help with the December 26, 2004 Indian Ocean tsunami provided a perfect vehicle for HFN research. Prior to the disaster, personnel were already scheduled to be in Thailand to plan for an upcoming technology demonstration with our Thailand Military coalition partners. In lieu of the pre-planned

events, the NPS faculty and contractors involved in the coalition field experiment program decided that this would be a perfect opportunity to further their R&D goals and help out the global community at the same time. As early as January 4, 2005, NPS personnel were on the ground planning and providing initial network support on the tsunami devastated coast of Thailand.

Initial efforts of the NPS HFN initiative began with the Wat Yang Yao morgue and grave registration center in the tin mining town of Takuopa, Thailand where over four thousand bodies and DNA samples were being processed. Additionally, a nearby survivor camp was enabled with broadband wireless to provide support to displaced victims, NGOs, volunteers, media, and others. This site supported over four thousand refugees, eight hundred families, and five hundred volunteers.

Even amidst the emergency situation, customs was an issue for some of the HFN equipment entering Thailand. Initially, support consisted of contracting a local satellite provider and extending connections through 802.11b wireless mesh nodes called BreadCrumbs from Rajant Corporation. This provided WiFi Internet connections to many users without them having to be near satellite connection. Within two hours of operating time the network had fifty to sixty users.

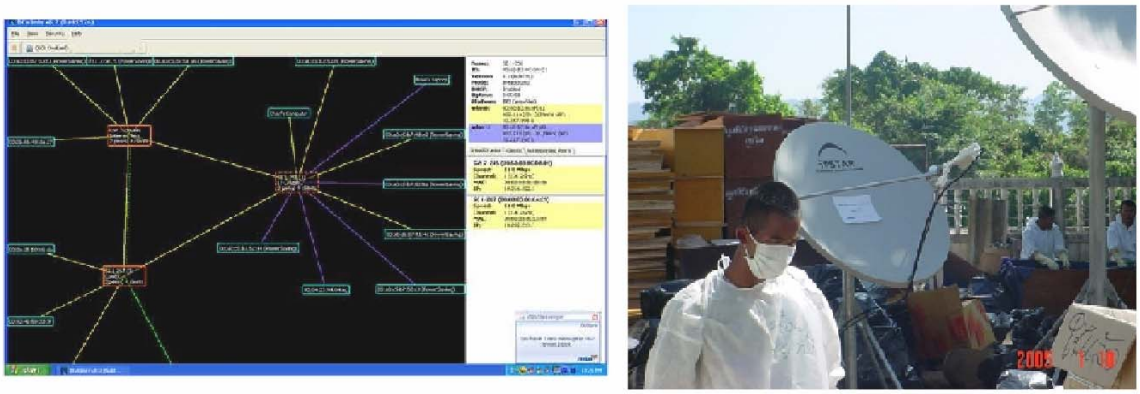


Figure 1. HFN at Wat Yanyao, Thailand

Subsequently, additional members of the HFN team were added and planning for longer term support began. After an initial site survey was performed, an HFN was constructed to support the two sites via a forensic dentistry office in Takuapa and the

survivor camp at Baung Muang. Personnel began returning from Thailand, and redeployment to the tsunami HFN sites was planned for February.

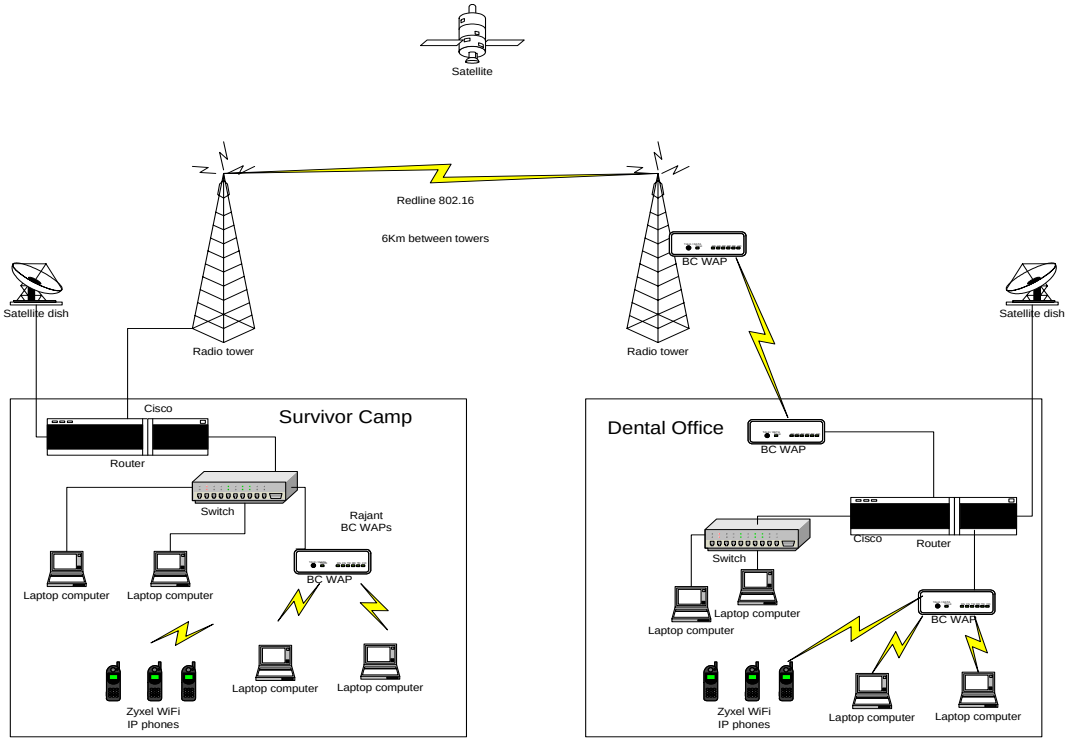


Figure 2. HFN to support Takuapa and Baung Muang Survivor Camp

Every effort was made to configure and test all gear prior to it being deployed to Thailand for operational use. Unfortunately, it was not possible to actually test the satellite links. Instead, additional PCs were used to substitute satellite connections to the Internet cloud. It was possible, however, to setup the entire bridge link on a smaller scale. Conducting tests prior to deploying the equipment allowed the team to be confident about the chosen solution. Routers were configured and tested to provide redundant Internet coverage if one of the satellite connections went down. This approach allowed the team to have eighty percent of the work done before arriving in Thailand.

Below are the configuration files for the survivor camp router and the dentist office router. Initially Network Address Translation (NAT) was setup to allow inside clients access to the Internet. Dynamic Host Configuration Protocol (DHCP) services supported internal clients, providing addresses, Domain Name Service (DNS) entries and

default routers. Finally, static default routes were used with weights to provide a redundant solution in case of satellite link failure.

```
!* Survivor.CiscoConfig
!* IP Address : 192.168.1.1
!* Community  : Tsunami
!* Downloaded 3/19/2005 11:33:49 PM by SolarWinds Config Transfer Engine Version 5.5.0

!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Survivor_Camp
!
enable secret 5 $1$yx8x$/O2/Jyebs8OlJNyrXZK1y0
!
ip subnet-zero
ip name-server 203.192.33.34
no ip dhcp conflict logging
!
ip dhcp pool 0
   network 192.168.1.0 255.255.255.0
   domain-name survivor
   dns-server 203.192.33.34
   default-router 192.168.1.1
!
!
interface Ethernet0
 description 10Mb connection from Survivor_Camp router to Survivor_Camp inside network
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 full-duplex
interface Ethernet1
 description 10Mb connection to Breadcrumb/802.16 for crosslink to Dentist
 ip address 192.168.3.4 255.255.255.0
 ip nat inside
 full-duplex
!
!
interface FastEthernet0
 description 10/100Mb connection to SaMart SatCom link ***not used yet***
 ip address 203.149.48.25 255.255.255.248
 ip nat outside
 speed auto
 full-duplex
!
!
ip nat pool survivor 203.192.48.27 203.149.48.28 netmask 255.255.255.248
ip nat inside source list 1 pool survivor
ip classless
ip route 0.0.0.0 0.0.0.0 203.149.48.25 10
ip route 0.0.0.0 0.0.0.0 192.168.3.4
```

```
no ip http server
!
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
!
!
snmp-server community Tsunami RW
banner motd _
Warning, Tsunami Relief Network!_
!
!
line con 0
 password 1qaz@WSX3edc
 login
line aux 0
 password 1qaz@WSX3edc
 login
line vty 0 4
 password 1qaz@WSX3edc
 login
!
!
no scheduler allocate
end
```

```
!* Dentist.CiscoConfig
!* IP Address : 192.168.2.1
!* Community  : Tsunami
!* Downloaded 3/18/2005 8:50:43 PM by SolarWinds Config Transfer Engine Version 5.5.0

!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Dentist
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$J4BW$2UyOsZjBZelQsCtI.cS7e1
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
!
!
no ip dhcp conflict logging
ip dhcp excluded-address 192.168.2.1
!
ip dhcp pool 0
   network 192.168.2.0 255.255.255.0
   domain-name dentist
   dns-server 203.192.33.34
   default-router 192.168.2.1
!
ip dhcp pool 1
   network 192.168.3.0 255.255.255.0
   default-router 192.168.3.2
   dns-server 203.192.33.34
!
ip cef
ip name-server 203.192.33.34
!
interface Ethernet0
 description 10Mb connection from Dentist router to Dentist inside network
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 full-duplex
!
interface Ethernet1
 description 10Mb connection to Breadcrumb/802.16 for crosslink to Survivor_Camp
 ip address 192.168.3.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 full-duplex
```

```
!
interface FastEthernet0
 description 10/100Mb connection to SaMart SatCom link
 ip address 203.192.51.10 255.255.255.248
 ip nat outside
 ip virtual-reassembly
 speed auto
 full-duplex
!
ip classless
!
no ip http server
!
ip nat pool dentist 203.192.51.10 203.192.51.15 netmask 255.255.255.248
ip nat inside source list 1 pool dentist
ip route 0.0.0.0 0.0.0.0 203.192.51.10 10
ip route 0.0.0.0 0.0.0.0 192.168.3.2
!
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
snmp-server community Tsunami RW
snmp-server enable traps tty
!
!
control-plane
!
banner motd _
Warning, Tsunami Relief Network_
!
line con 0
 password 1qaz@WSX3edc
 login
line aux 0
 password 1qaz@WSX3edc
 login
line vty 0 4
 password 1qaz@WSX3edc
 login
!
end
```

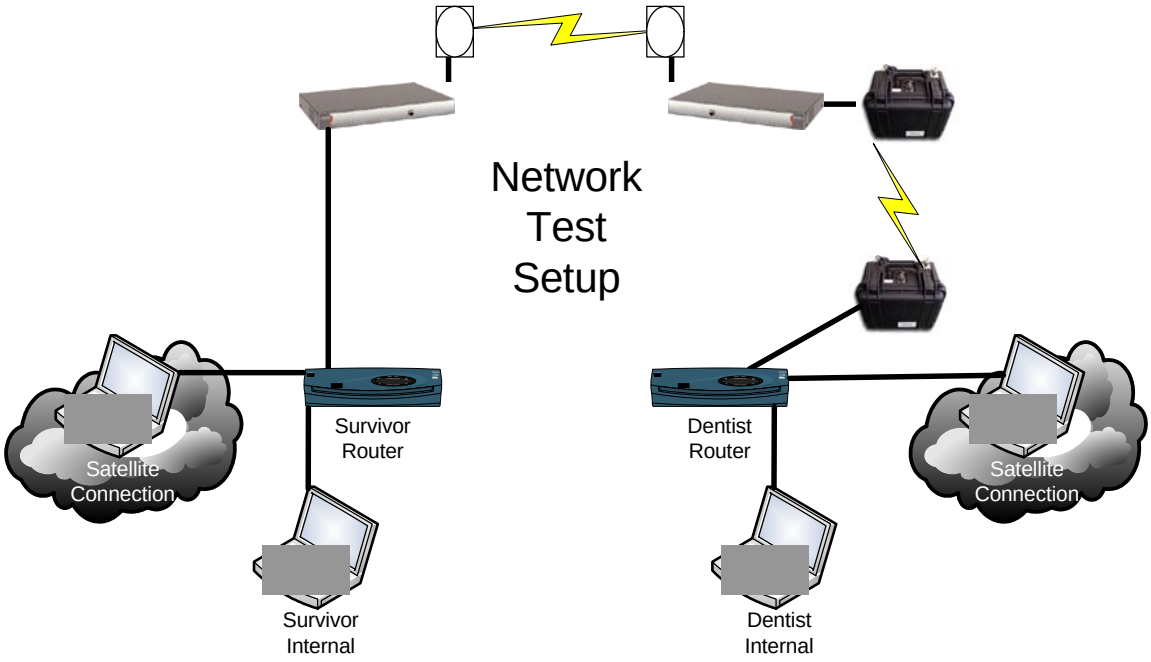


Figure 3. HFN network test setup

Basic connectivity tests were conducted by pinging interfaces. The routing was tested by unplugging cables to simulate an interface failing. The test run was successful and configurations were saved for transport. It is very important to copy the running configuration to the router prior to turning it off. If this is not done, the router will not have the same configuration when it is turned back on. This can be a source of frustration, especially once everything is in the field.

SolarWinds Cisco Tools were then used to access the routers through SNMP. Notice in the configuration files that the SNMP server is set with an access string of "Tsunami" with privileges set to read and write. This was a convenient way to configure the routers remotely. However, there were some security concerns using SNMP version 2. The most secure configuration option is to program the routers through the console port. This is not a remote option though. Other available options are command line interface (CLI) through SSH access, SNMP version 3, and HTTPS configuration over SSL.

Several changes had to be made once the equipment actually got into Thailand. For starters only one satellite connection was acquired and all of the IP addresses were

different. This small setback required personnel locally to set up the interface connecting to the satellite connection first before any remote configuring could be accomplished.

The following list of lessons learned is provided:

- Take plenty well labeled crossover cables for connecting like devices.
- Ensure that on site personnel have console cables and can at a minimum set IP addresses for router interfaces.
- Plan out power for all devices. Not doing so will result in damaged equipment.
- Plan to carry as much of the equipment as possible. Shipping gear resulted in time delays with customs.
- Use USB GPS with computers for convenient device locations.
- Helium balloons work well for assisting in aiming distant antennas.
- Plan for secure remote management because details will always change.
- If possible, have a means of communication with personnel at each site.
- Keep deployable equipment up to date with firmware and patches.
- Deploy with sustaining equipment. For instance, bring water proofing, lightning arrestors, and power filter/stabilizers.
- Pre-configure as much as possible prior to departing.
- If a feature on a device is not needed, turn that feature off. For example DHCP services, mesh routing, etc.
- Carry electronic and paper copies of configuration files. Also, use those assets and resist changing things at the site. Usually the tested configuration will be more reliable than spur of the moment ideas.
- Document configuration files as much as possible. This allows on site personnel to have more information about the configuration.
- Create active CDs for standardizing computers. These CDs are bootable operating systems that can be configured and distributed to provide standard systems. Knoppix is an example (knoppix, 2005).

III. GENERAL CONFIGURATION OF A HA/DR HFN

There are three main components that meet the requirements for an HFN. These components are a reach-back connection to the Internet or possibly a headquarters, last mile connections to other sites, and the connecting network devices in between. The FLAK is presented by this thesis as an example of a compact node which provides flexible and multiple connections.

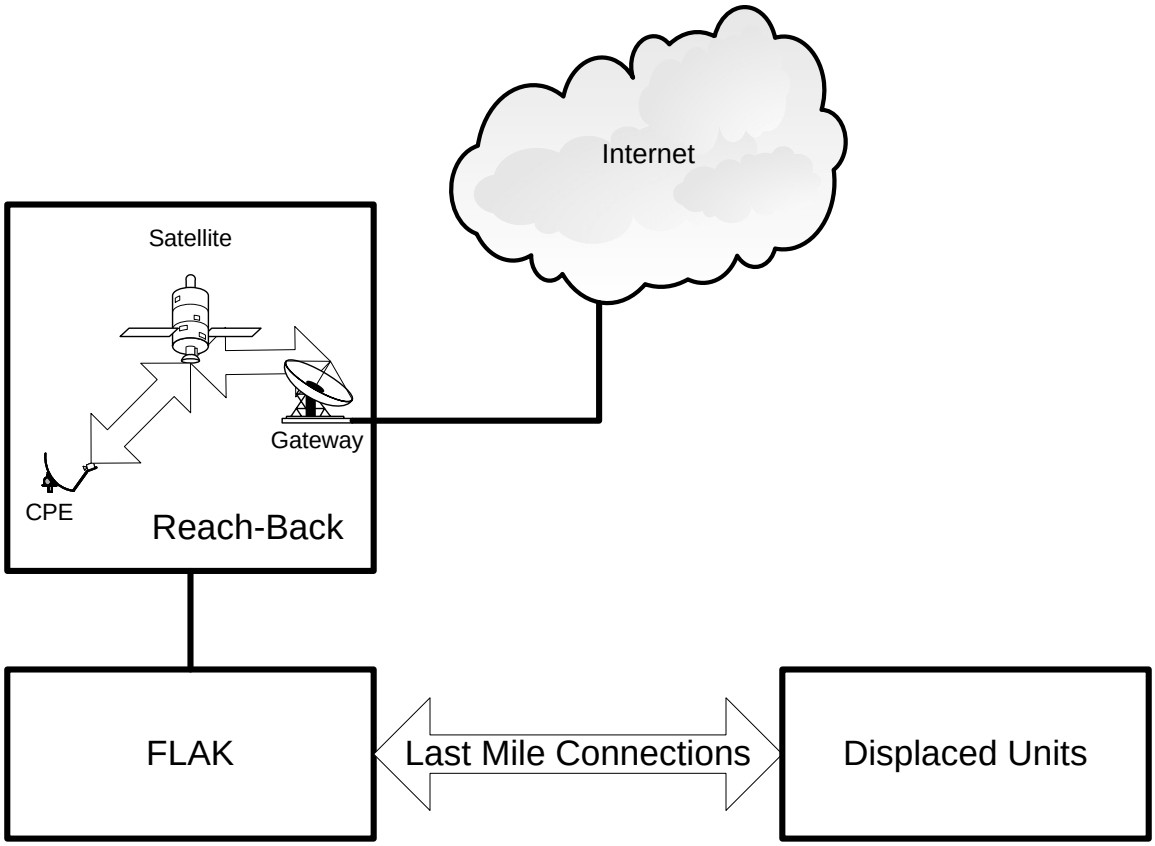


Figure 4. Three Basic HFN Components: Reach-Back, Last-Mile, and FLAK

Commercial satellite is just one example of a reach-back connection. Other solutions include terrestrial fiber, serial, or DSL connections. This thesis focuses on commercial satellite because it meets the mobility and availability requirements of an HA/DR HFN. A reach-back connection is the main connection that links a remote site to

the rest of the world. The remote terminating end of the reach-back is normally referred to as a point of presence. The FLAK in this case is the point of presence node.

Last-Mile connections are links from the FLAK to displaced units through out the area. These connections are needed due to limitations of the displaced units with respect to reach-back, and to maximize use of the broadband connection to the FLAK. Solutions for last-mile connectivity should be flexible and easily moved or changed. For this reason, most last-mile connections are wireless. Chapter V covers last-mile connections in more detail and lists several examples.

The FLAK is the collection of equipment that supports flexible connections between the reach-back solution and the last-mile solution. Its primary goal is to remain very mobile while supporting multiple connections and some applications. Ethernet is the current desired interconnectivity with other devices.

IV. SATELLITE REACH-BACK CONNECTIONS

A. OVERVIEW

Many different solutions exist to provide Wide Area Network (WAN) connections to users. It is inherent upon the responding agency to weigh the pros and cons of different systems in order to meet requirements within the available budget. The flexibility, responsiveness, and capabilities of satellite communications make it a primary choice for remote areas. Commercial multi-channel satellite systems are becoming more available and current advances make satellite solutions more affordable and effective. This section will cover a category of satellite terminals that provide broadband connectivity, Very Small Aperture Terminals (VSATs).

B. VSAT SYSTEMS

Most satellite systems are made up of similar smaller subsystems that include remote terminals, a satellite, a terrestrial hub, and additional terrestrial infrastructure. The customer premise equipment (CPE) is general terminology that refers to the equipment located with the user which normally consists of an outdoor unit (ODU) and an indoor unit (IDU) (Tachyon Networks, 2004). This equipment comes in various different shapes, sizes, and means of employment.

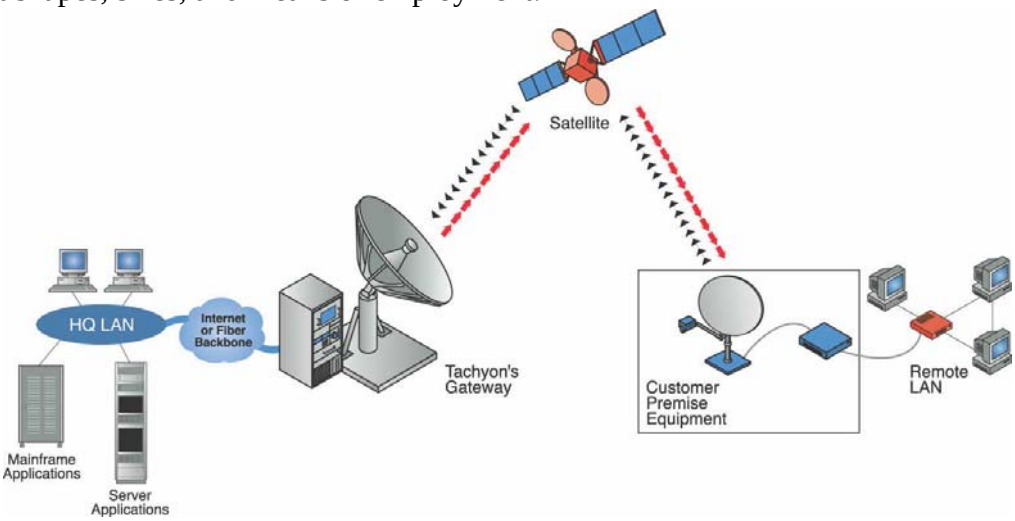


Figure 5. Example of a VSAT solution (from Tachyon, 2004)

C. FREQUENCY

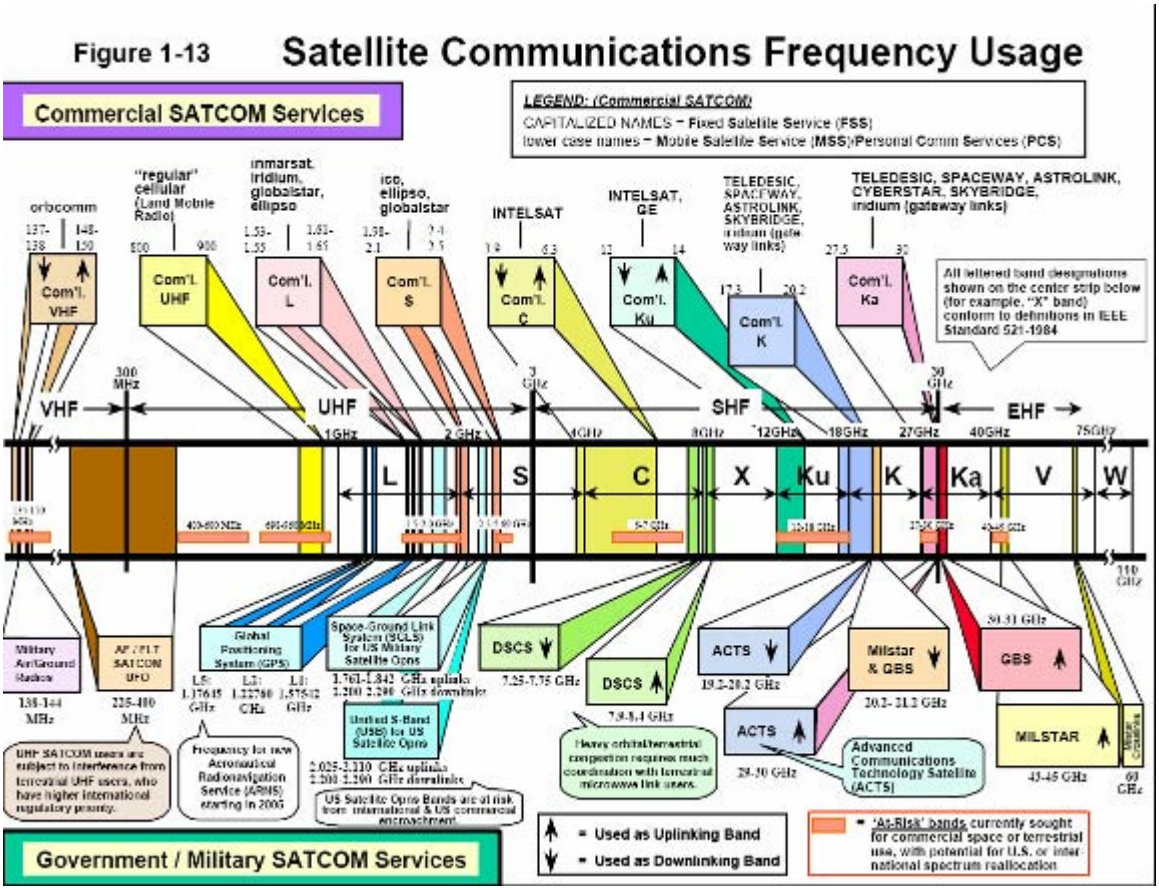


Figure 6. Satellite Communications Frequency Usage (From Headquarters, Department of the Army. (2000). *The Army satellite communications architecture book. Fort Gordon: TRADOC*)

The chart in Figure 6 above shows frequency spectrum use by military and commercial systems. Most VSAT systems use the Ku spectrum. Ka is also used but unfortunately, the Ka-band signal wavelengths are so short that moisture droplets can absorb and depolarize the Ka-band signal, meaning rain, snow, or even rain-filled clouds passing overhead can attenuate the incoming signal.

D. NETWORK TOPOLOGIES

There are three primary topologies deployed for satellite solutions: Point to Point, Star, and Mesh. Sometimes these topologies will be combined and referred to as a hybrid topology. The implementation used will depend on the type of service that is to be provided as well as the information exchange requirements. Additional elements that

influence a topology will depend on the desired services, security, end users, throughput required, and capacity.

1. Point to Point

Point to point communications closely match the performance of terrestrial WAN connections. Normally point to point topologies use a single channel per carrier, which can support high data rates. The requested rate is always on and dedicated to the user. This type of connection is ideal for all types of voice, data, and video traffic, but is an inefficient use of satellite bandwidth for burst transmissions.

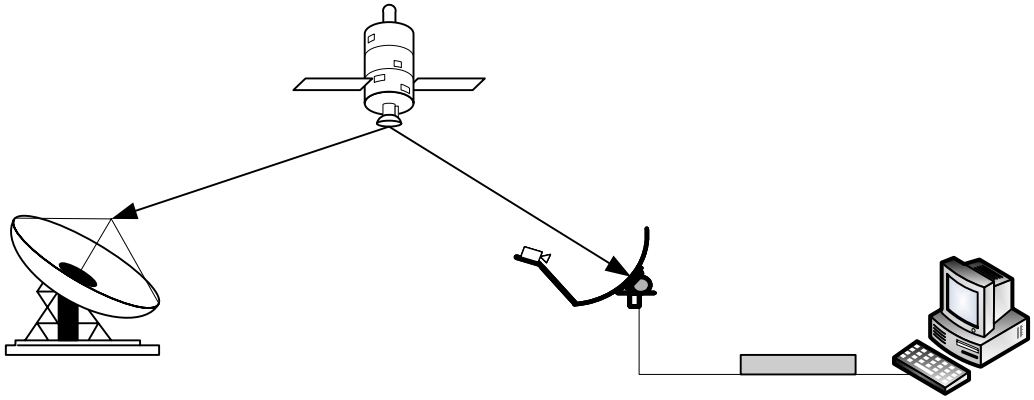


Figure 7. Point to Point Topology

2. Star

Star topology is used when many terminals have traffic that terminates at a designated earth station, like a headquarters. In this case all traffic to and from remote terminals must be routed through a central gateway or hub. Earth stations are simple and less expensive because they do not have to deal with routing to other network nodes. In Star topology, the central hub is responsible for the routing. Typical uses for Star topology networks are corporate networks with a headquarters and remote offices, credit card verification services, and inventory monitoring.

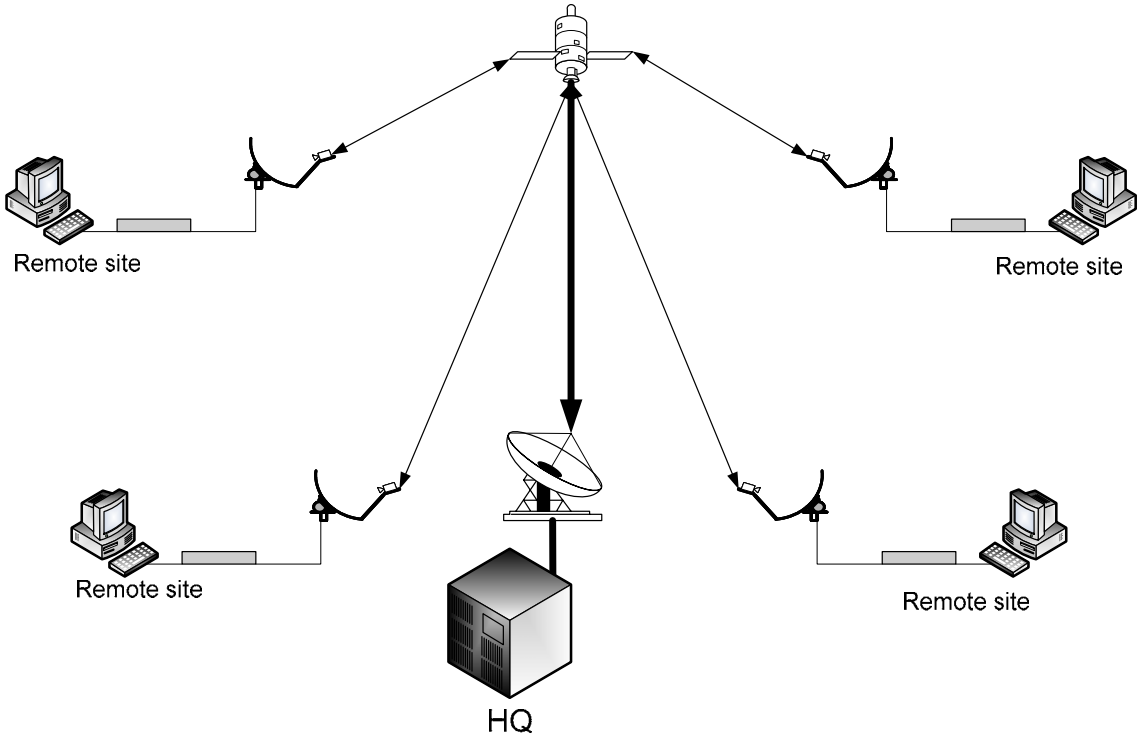


Figure 8. Star Topology

3. Mesh

In a Mesh network end users have connection paths for direct communication with each other. These connection paths are accomplished with single relays through the satellite. This reduces the number of hops between end users compared to a Star topology and reduces time delay for applications. Star and Mesh topologies can be combined in various ways. For example, some of the sites can be configured as hubs in a Star network and the remaining sites as a Mesh network. Alternatively, a VSAT may be part of a Star network and part of a Mesh network concurrently. The combination selected depends on whether the applications used require a Star or Mesh topology.

E. OUTDOOR UNIT (ODU)

1. Antennas

VSATs are relatively small and refer to the most visible part of the system -- the antenna assembly which is normally around .75 to 2.4 meters. Smaller antennas are desirable for mobile, rapid deployable systems, but the antenna size depends on several

different variables. Frequency range, satellite footprint, power, and desired connection speed all affect the size of the antenna.

While some systems can take advantage of omni-directional antennas for use in communicating with a satellite, they are mainly “receive only” systems. The size of the antenna will be proportional to the size of the wavelength for the corresponding frequency. GPS is a primary example of this type of system. However, it is conceivable that Common Operational Picture (COP) applications could use this to receive information as well.

The most commonly used type of antenna for satellite systems is one with a parabolic reflector. Its operation is derived from optical physics and is possible due to microwaves being in a transition region between ordinary radio waves and infrared/visible light (Carr, 2001). Figures 9 and 10 below show the two broad categories of parabolic antenna: center fed prime focus and Cassegrain fed. Additionally, there are some modifications of these types.

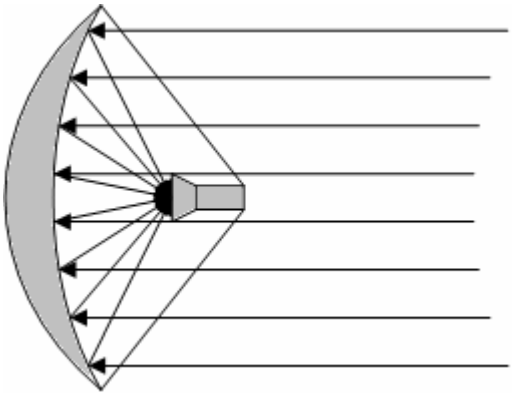


Figure 9. Center fed prime focus parabolic antenna

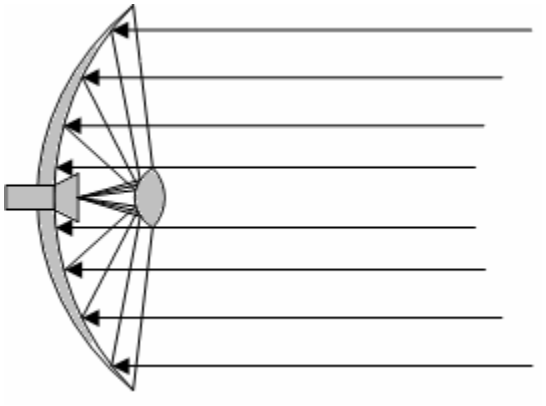


Figure 10. Cassegrain fed

Parabolic antennae with a focal point directly at the front and center of the reflector are called center fed prime focus antennae. These antennas are easy to construct and point directly toward the desired satellite. However, there are two main design disadvantages:

- The feed horn and supports block part of the reflector surface.
- The feed horn is subject to greater interference from heat.

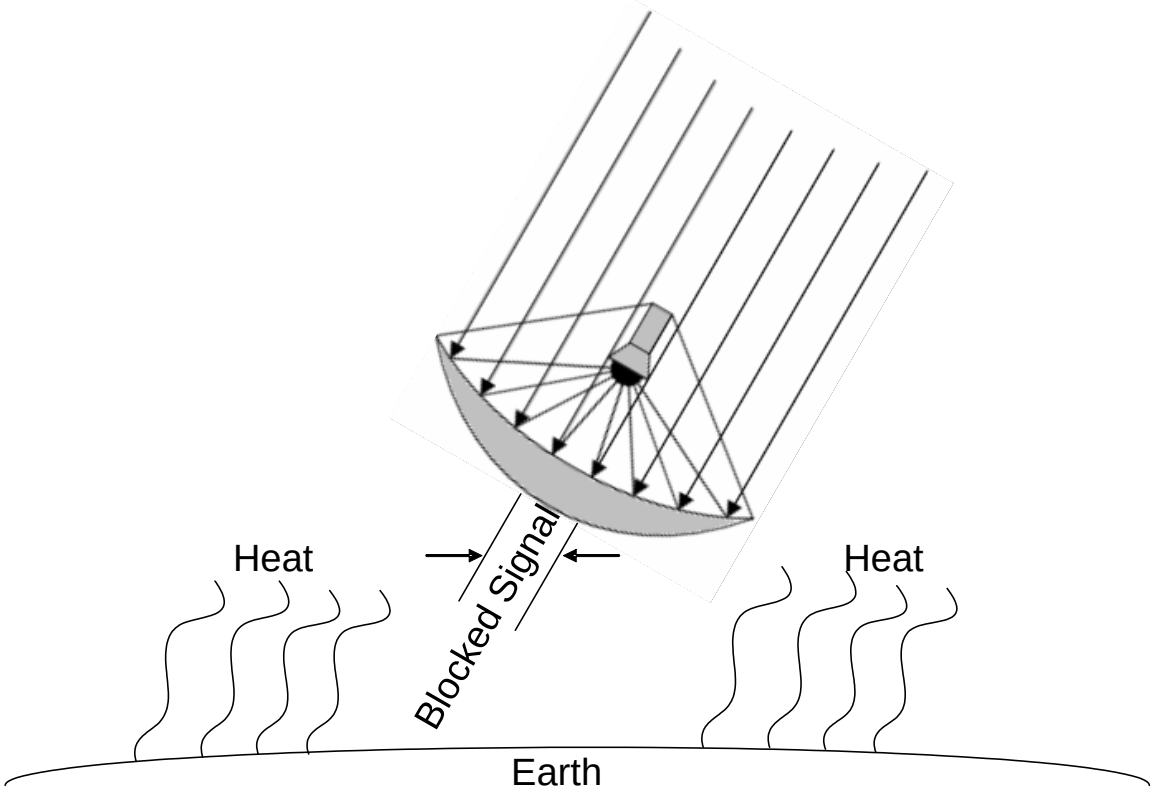


Figure 11. Disadvantages for center fed prime focus antenna

While the hardware blockage is self-explanatory, the interference from heat requires some explaining. Normally the ground is in position behind the antenna and the ground emits heat that can affect the operation of the antenna. The affect of heat changes the noise used in the link equation and can reduce the antenna's efficiency. This effect is greater closest to the edge of the antenna and requires calibration of the feed horn for transmission so that the illumination of the antenna is tapered to minimize noise contribution from the perimeter of the dish.

Larger parabolic antennae tend to use the Cassegrain design. The Cassegrain design incorporates a small sub reflector located at the front and center of the dish. This reflector redirects signals back toward the center of the dish, where the feed horn is mounted. The Cassegrain suffers from blockage issues just like the prime focus. This blockage is very small compared to the size of the parabolic dishes, which can be large. The feed horn on Cassegrain antennae is pointed toward the sky and is more efficient since it is not affected by the heat of the Earth as much.

Today the popular dish design for VSATs is a parabolic antenna called an offset focus antenna as shown in Figure 12. This type of antenna has the feed horn positioned at the bottom of the dish. In this case, there is no feed horn blockage – an important consideration when the antenna aperture is less than one meter in diameter. Also, the offset angle at which the feed horn tilts up toward the reflector is such that if the feed looks over the antenna's rim it will see the cold sky rather than the hot earth. Due to these advantages, the offset-fed antennae can achieve higher efficiency levels than prime focus antennas can generally attain (Carr, 2001).

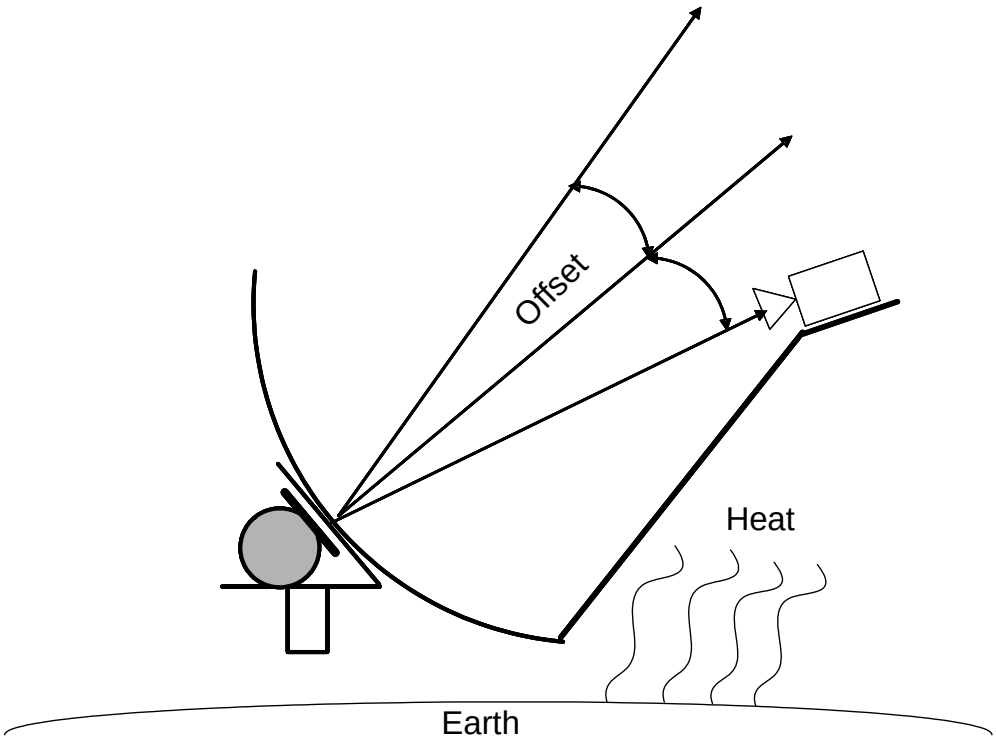


Figure 12. Example of offset focus antenna

2. Radio

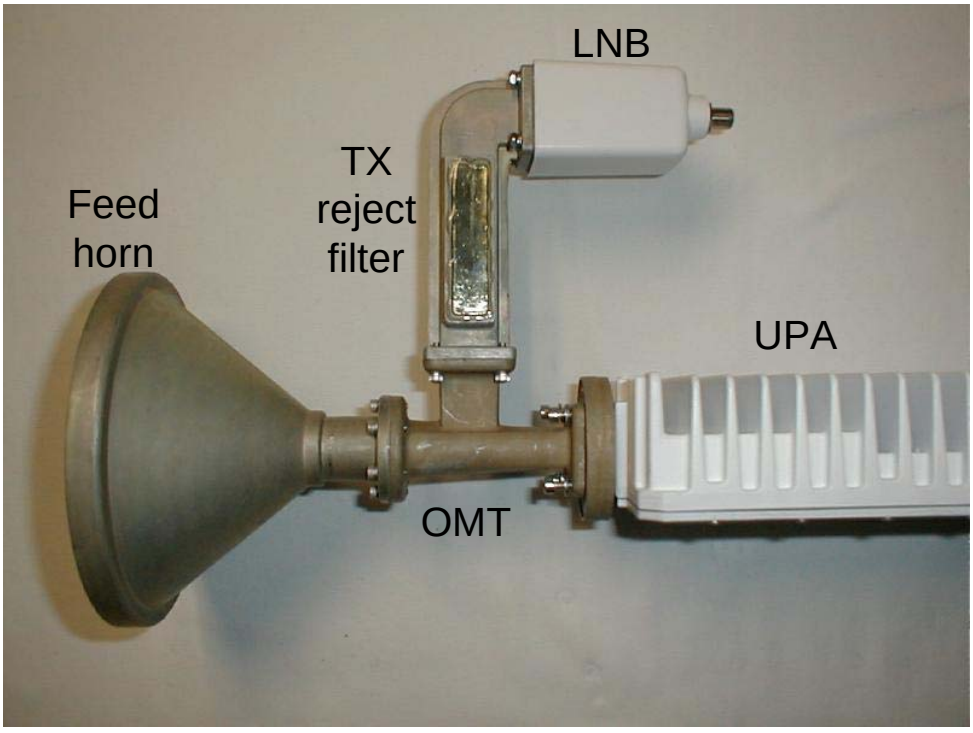


Figure 13. Satellite radio components

The radio portion of the antenna is made up of five main parts: feed horn, ortho-mode transducer (OMT), transmit reject filter, low noise block down converter (LNB), and the up converter power amplifier (UPA). Each piece has a specific responsibility in transmitting and receiving signals.

The feed horn is the antenna focal point. It effectively collects or emits the received and transmitted signal respectively. Figure 13 displays an example of a feed horn that is used for a center fed prime focus or offset focus system. It is easily identified by its conical shape and has a drum-like surface.

The OMT is used to separate transmit and receive signals. It accomplishes this by the inherent shape of the waveguide form that is found inside of the actual OMT. Figure 14 shows an example of the different wave guide orientations. This design facilitates frequency reuse by taking advantage of orthogonal properties of signals. The demand for radio frequency (RF) spectrum far exceeds that which is available. Using transmit and receive signals of the same band with different polarity helps achieve better frequency reuse.

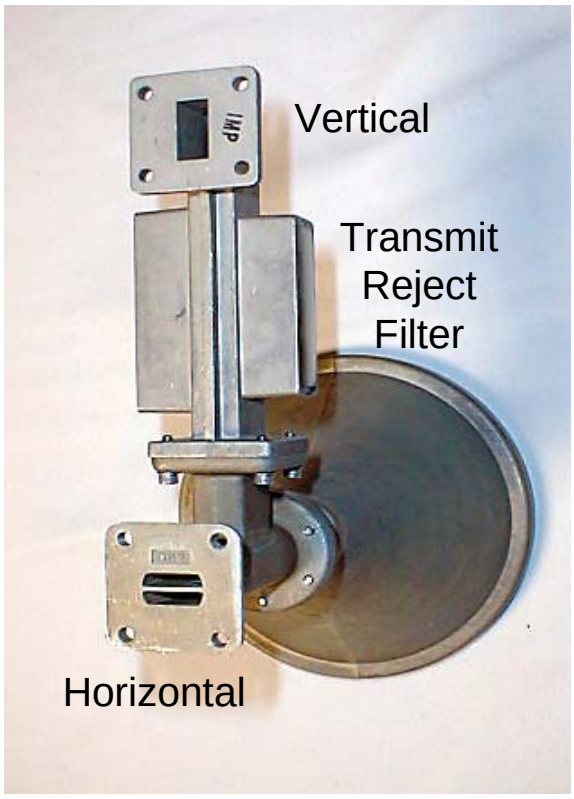


Figure 14. OMT and transmit reject filter wave guides

Power is a great concern with respect to the satellite itself. For this reason, signals that are transmitted from the satellite are not very powerful. This creates some concerns in attempting to receive a signal on the ground. The transmit/reject filter is positioned to remove unwanted signals prior to frequency conversion and amplifying of the received signal.

The LNB is part of the receiver system. Its primary job is to down convert the received signal to a frequency that will be accepted across the coaxial cable and the IDU's modem. The standard for North America is an 11700 - 12200 MHz type digital LNB that uses a 10750 Mhz frequency oscillator.

Last is the up-link converter power amplifier. The UPA is the transmitting radio for the satellite. It converts the signal to the appropriate uplink frequency and amplifies the signal. Next the signal is polarized as it passes through the OMT.

F. CHANNEL ACCESS TECHNIQUES

This section will cover three of the more popular access control techniques. Demand-Assigned Multiple Access (DAMA), Time-Division Multiple Access (TDMA), and Single Channel Per Carrier (SCPC). Selection of a specific access technique will depend on the applications, traffic profiles, and the tolerance for delays.

1. Demand-Assigned Multiple Access (DAMA)

Increased use of satellite communications has quickly saturated the capacity of available frequency space. DAMA channel access solutions are used to share bandwidth through automated channel sharing. Channel resources are allocated on the basis of current needs and network rankings. This type of channel access provides a central control mechanism and access provided by a scheduling MAC.

2. Time-Division Multiple Access (TDMA)

TDMA is a static multiple access technique where the channel is broken down into time slots. This sets up each user with the full bandwidth of the channel for a given time. TDMA does not adapt to changing traffic loads and unused time slots become

wasted channel resources. Discussion later covers 802.16 which uses a combination of both DAMA and TDMA.

3. Single Channel Per Carrier (SCPC)

SCPC supports true multimedia capabilities: voice, data, fax, and e-mail. It is frequently used from broadcast systems. SCPC should be used when users require guaranteed bandwidth. Some advantages of SCPC include simple and reliable technology, low cost of equipment, high data rates, and ease of adding additional receiving sites. It has as its greatest disadvantage the inefficient use of satellite bandwidth for an IP network. This type of access resembles a circuit switched network.

G. INDOOR UNIT (IDU)

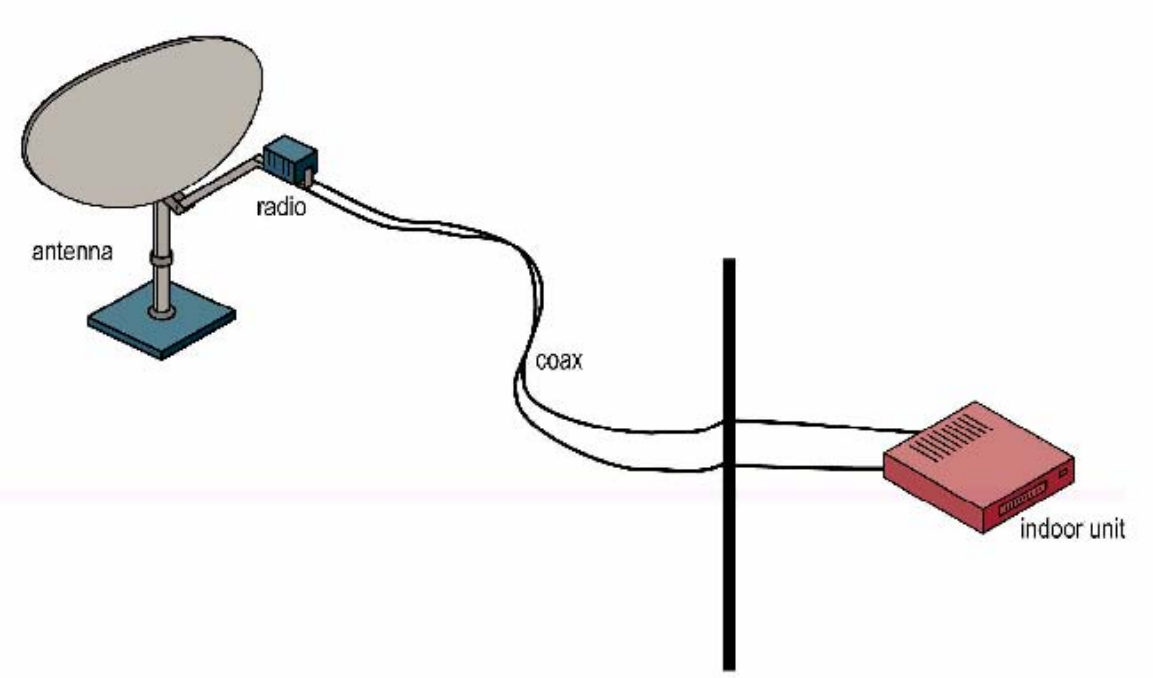


Figure 15. ODU and IDU (From Tachyon Networks, 2004)

As shown in Figure 15, the IDU is connected to the ODU by two coaxial cable leads, one for transmit and one for receive. The IDU houses the satellite modem, provides power to the LNB, provides power for the UPA, and provides an Ethernet

connection for IP devices. Typical installation for the IDU is a nineteen inch, one rack unit device. Most devices support switching power supplies for 100—240 VAC and 50—60 Hz.

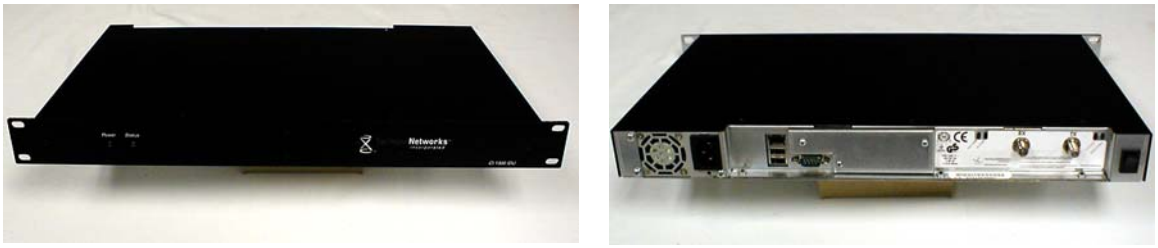


Figure 16. IDU

H. ADVANTAGES OVER TERRESTRIAL CONNECTIONS

Satellite solutions have several advantages over competing terrestrial technologies. A primary advantage is capacity sharing on the satellite. This is allowing satellite solutions to approach comparable prices with leased lines. Other advantages include:

- Natural broadcast capability and Multicast support. Data can be distributed in a very fast and cost-efficient way by sending it simultaneously to multiple receiving sites.
- Easy implementation. Incremental user locations can be added to a network quickly and cost effectively without interrupting network usage.
- Geographic flexibility.
- Single vendor solutions. Vendors can normally support a much larger area that can span national borders.
- Uniform network services. Users are not limited to terrestrial connections for their area.
- High network availability. Supports regions that have a poor terrestrial telecommunications infrastructure.

I. CONCERNS FOR TCP CONNECTIONS

While the performance of a transport protocol is important, it is not the only consideration when constructing a network containing satellite links. For example, data link protocol, application protocol, router buffer size, queuing discipline, and proxy

location are some of the considerations that must be taken into account. The following characteristics of satellite channels may degrade TCP performance:

- Long feedback loop due to the propagation delay being approximately half a second.
- Large delay * bandwidth product leading to a large number of packets in flight but not acknowledged.
- Transmission errors due to higher bit error rate signaling network congestion.
- Asymmetric use due to the uplink having less capacity than the downlink (Allman. 1999).

MTU discovery and Forward Error Correction (FEC) are elements at the data link layer that can improve TCP performance. These interactions are not well understood and require additional research before improvements can be certain. MTU discovery relates to sending bigger frame segments which in turn should mean more data sent with less TCP overhead. FEC attempts to improve the Bit Error Rate (BER) providing a better connection over the satellite link. This procedure decreases the amount of lost information. TCP's inherent nature is to treat packet loss as the result of a congested network. Dealing with satellite links or radio links in general, this is not always the case. Providing a means to reduce lost data in turn mitigates the effects of TCP retransmissions (Allman, 1999).

Congestion control algorithms are discussed in RFC 2488 that deal with satellite communications. These are beyond the scope of this thesis, but are listed below for information.

Slow start congestion avoidance is a control algorithm implemented in order to prevent a station sending data from sending an overwhelming rate of data on the network. Because the transmission speed of the link is not initially known, the station will tend to ramp up until a maximum supported speed is reached. Often the latency over the satellite link will cause the sending station to wait for acknowledgements and interpret this as a slow link.

Next, throughput is limited because of the affect the Round Trip Time (RTT) for a signal traveling to and from a geosynchronous satellite. Throughput is defined by the following formula:

Throughput = window size / RTT (Allman, 1999)

Since the window size is limited by TCP, an increase in the RTT will result in a decrease in the throughput. This is not a desired result. Efforts can be made to increase the window size and lessen the affect of a large RTT.

Commercial providers like Tachyon and others have implemented solutions within their network to attempt mitigation of the effects. Answers have come in the form of proxy servers, improving BER, through the use of selective acknowledgements (Tachyon, 2004).

Additionally, several commercial companies have specialized in providing hardware link accelerators and software performance enhancing protocols (PEPs) that assist in communicating over satellite links. SkyX, ComTech, Expand, and Peribit are examples of vendors that are providing these types of solutions.

Figure 17. Expand link accelerators for JWICS, SIPRNET, NIPRNET (from Dataline Incorporated, http://www.dataline.com)

V. LAST MILE CONNECTIONS

A. OVERVIEW

Once a connection has been established locally, the desire is to distribute this connection to other networks and users. This is commonly referred to at the last mile. Typical commercial examples have been answers to deliver fiber-like speeds to locations quickly and without the expense of laying actual fiber. Solutions include free-space optics, 802.11 Wifi, and 802.16 WiMax.

B. FREE SPACE OPTICS

Free Space Optics (FSO) has the ability to deliver connection speeds from 100 Mbps to several Gbps. The data is transmitted over lasers point to point and can function over several kilometer distances. FSO is an optimal solution for point to point links in areas with consistent fair weather. Typical solutions are building to building connections that are cheaper than providing a fiber connection. See Table 1 below for an overview against other options.

C. WIRELESS 802.11 (WIFI)

WiFi exists as a possible means for last mile extensions. It was not inherently designed to perform over large distances, but has the ability to provide connection options including: client/host, peer-to-peer (ad-hoc), point-to-point, point to multi-point, site-to-site bridge, or last mile connections. WiFi is a direct sequence spread spectrum solution that operates in the 2.4 GHz frequency range. Multi-path interference and unintentional jamming can cause significant problems for a WiFi solution.

D. WIRELESS 802.16 (WIMAX)

WiMax is part of a solution dubbed as “fixed broadband wireless.” It uses orthogonal frequency division multiplexing (OFDM) which provides resilience to multi-path and noisy environments. While not particularly reliable, 802.16 offers some non-line of sight abilities. Despite any minor troubles, 802.16 provides a robust solution for last mile implementations.

UOC/CAC2S/CoNDOR	Distance	Pros	Cons
FSO	LOS	Fiber throughput speeds, quick setup time, operates in license free spectrum	Susceptible to weather conditions, short distance (< 5 km), laser alignment
MICROWAVE (RFM)	LOS	Up to OC-3 speeds, already packaged, reaches out to 13 kilometers	Obtain authorization for frequency use, susceptible to interception due to RF use
802.16	LOS	Adaptive modulation, up to 66 Mbps, 360 degree coverage out to 20 km	No built-in encryption, company evaluated was ATM based (there are others IP based)
802.11b over SecNet-11	LOS	Type 1 encryption built-in, send up to secret level data, small footprint	Low throughput of 1-2 Mbps, difficult to configure, not compatible with other 802.11b
OFDM	BLOS	Communicates over hills, through trees, and around buildings, 25 Mbps throughput	Limited encryption built in, need good azimuth for BLOS connectivity
BROADBAND SATELLITE (Segovia/Omega Systems)	BLOS/OTH	Large throughput capabilities of up to 9 Mbps, mountable on a vehicle, Type 1 encryption	Annual/Monthly Fees, but not by minute
INMARSAT (Nera)	BLOS/OTH	Satellite connectivity on-the-move, small mountable vehicle platform, encryption	Expensive per minute fees, low throughput of 56 Kbps (working on upgrades)
IRIDIUM	BLOS/OTH	Capable of combining four channels, comms on-the-move, no monthly fees	Low throughput of 2.4 Kbps per channel, difficult to send data without compression

Table 1. Technology Summary (From Garcia and Joseforsky, 2004)

E. DISCUSSION

The author, along with other NPS faculty, students, and General Dynamics, conducted wireless testing of the above technologies in January 2004 in Scottsdale, Arizona. Multiple wireless technologies were tested in last mile scenarios for ease of implementation, bandwidth measurements, and application support ability. Table 1 is a consolidation of the overall impressions of each.

While the testing distance was only one kilometer, the test provided extensive data on link and application performance. Cisco CallManager was implemented as a VoIP solution with Cisco 7960G phones. Various data transfers and video applications were used to test and tax the network. Figure 18 shows a diagram of the network setup and some of the applications tested.

Redline Communication's WiMax solution has been the predominant last mile technology with which the author has worked. Tasks have been multiple hops to connect NPS with the Camp Roberts test facility one hundred miles South of the school, a six kilometer Thailand HFN link, and connecting the Fort Ord MOUT facility to additional TNT networks. The WiMax gear has been a very reliable means of last mile connectivity

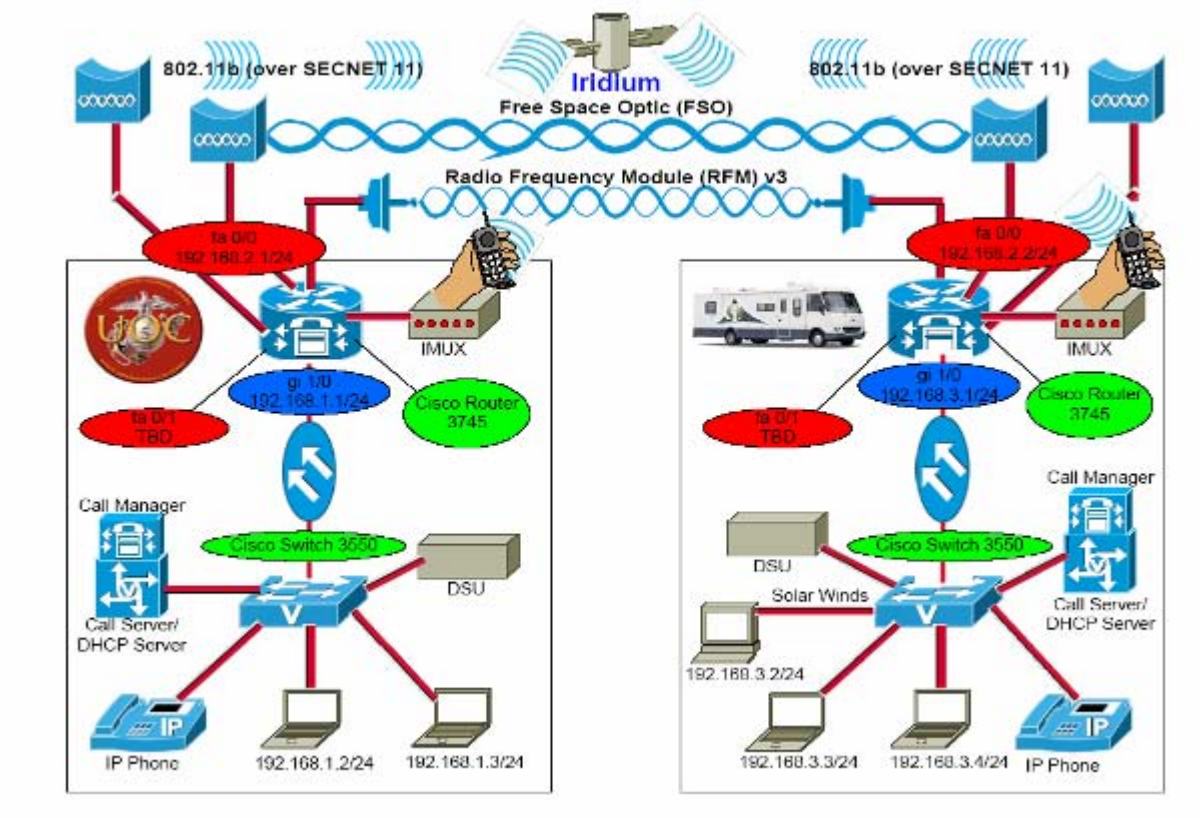


Figure 18. General Dynamics Testing Network Diagram (from Garcia and Joseforsky, 2004)

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCEPT OF A FLAK

A. OVERVIEW

The idea for designing a FLAK is not a new idea. The Contingency C4ISR Handbook for Integrated Planning (CHIP) covers current systems in use and the services that they provide. The purpose of this research, however, is to explore what equipment is needed to support a command and control node for civil-military efforts. As mentioned earlier in this thesis, many times even the unclassified realm is not readily available to all types of personnel in an emergency or relief environment. For this reason a solely commercial off the shelf (COTS) approach was taken.

Additionally, some of the implementations are not in use or accepted for military operations at the present time. It is the author's opinion that research in this area will help to mature these solutions and promote awareness for a military audience. The use of commercial satellites, virtual local area networks (VLANS), voice over Internet protocol (VoIP), and emerging wireless technologies are examples that this section will cover.

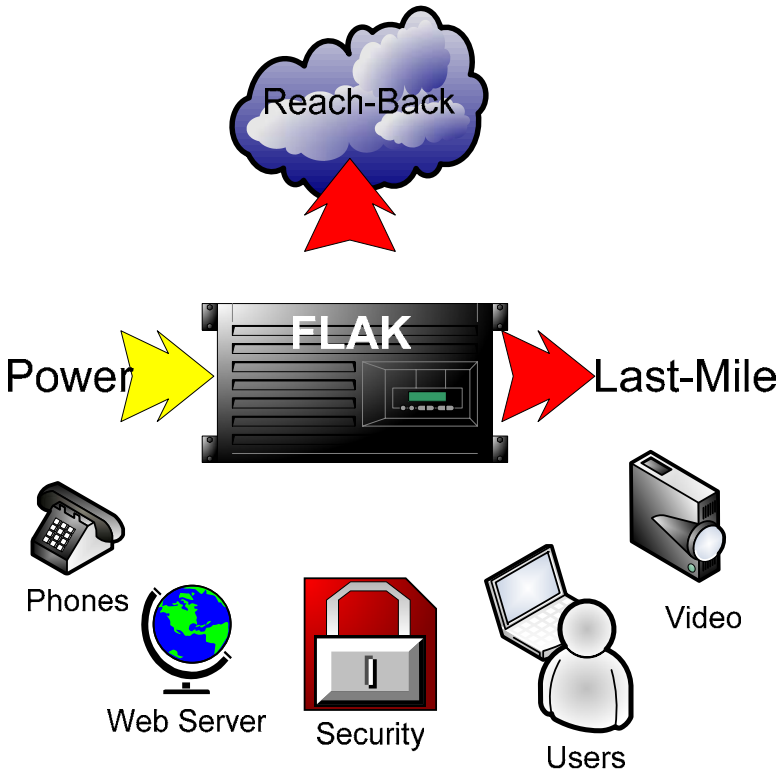


Figure 19. Functional FLAK Diagram

Figure 19 shows a functional diagram of the FLAK. This diagram is provided to offer a better visual of the inputs and outputs for the FLAK. Voice services are provided by the FLAK with VoIP and connections to the PSTN. Additional services and applications can be supported as shown.

There are also several commercial companies that are working on providing this same type of solution to civilian and military organizations. Cisco Systems is designing a Mobile Commander's Kit that is a smaller, customized version of the FLAK. Telecommunication Systems (TCS) provides the SwiftLink series of products that are rapidly transportable, support SIPRNET and NIPRNET, and certified encryption, but are designed to use the lower bandwidth Inmarsat satellite network. Dataline Incorporated has several ultra-lite packages that will support different WAN connections.

B. POWER

Power is a major concern for any equipment planned to deploy into remote areas. Solutions vary from batteries to solar to generators to existing infrastructure at the HA/DR site. Each power solution has concerns and possible limitations that must be considered when planning. Table 2 is provided for general power planning guidelines concerning the FLAK.

Equipment	**Power in Watts**
Tachyon Satellite CPE	180 (max)
Cisco 2811 Router	210 (max)
Redline AN50e	120 (max)
MeshNetworks Intelligent AP	120 (max) estimated

Table 2. Power requirements for the FLAK

1. Battery Power

Batteries offer a very attractive solution to the mobile user. A battery solution allows the FLAK to move freely without the hindrance of being tied to a stationary power

source. However, a power inverter is required to support the FLAK in its current state. DC versions of equipment used in the FLAK are available, but it is easier to use the standard equipment with batteries and an inverter. This type of implementation supports running off common vehicle batteries.

2. Solar Power

A solar power solution can be used also. This type of solution is used normally in conjunction with a battery power solution. Items to consider when using solar power are size, weight, and preventive maintenance. A solar installation may weigh several hundred pounds and require a large space. Not being dependent on AC power is this solution's obvious advantage. Solar power is particularly beneficial in an remote emergency situation.

3. Generators

Generators are really a family of solutions based on the type of fueling system for the generator itself. Solutions include, but are not limited to gasoline, diesel, and hydrogen fuel cell. Each type of generator has advantages or disadvantages that must be weighed for the situation.

a. Gasoline

Modern gasoline generators are produced by many companies and offer very efficient power solutions. Experimentation and demonstrations conducted with the FLAK in remote areas were powered by a Honda EU2000i gasoline powered generator. The current implementation of the FLAK uses approximately one quarter of the 2000 watt rated power from this type of Honda generator. Under such a load, the Honda EU2000i can operate for about fifteen hours.

Figure 20. Honda EU2000i generator

Advantages for this type of power solution include: lightweight, compact, quality power output, low fuel consumption, and quiet operation. The greatest disadvantage is probably the reliability of gasoline in remote or disaster stricken areas where fuel for the generator itself may not be available. Certain environmental conditions can affect the feasibility of refueling generators as well.

b. Diesel

Diesel generators are common industrial type solutions. These generators are large, heavy, and would be hard to transport. Most diesel generators support tens of kilowatts or more and would supply more than enough power for the FLAK. An additional advantage is the availability of diesel in the HA/DR environment. A large amount of military equipment is reliant on diesel power. This could increase the availability of diesel in an environment where other fuels are not available.

c. Hydrogen Fuel Cell

The Wireless Warfare Lab at NPS has a hydrogen fuel cell generator that has been used in remote sites for power. While this is an alternative fuel source that could provide power, it is bulky and heavy. It is questionable if hydrogen fuel would be available to recharge cells in a HA/DR environment.

d. Other

Other solutions for generators include: natural gas, propane, and tri-fuel generators. Natural gas and propane generators are more commonly found as fixed installations for backup power solutions. Tri-fuel generators are similar to the gasoline

models covered above. The success of all generator solutions are subject to the availability of fuel in the HA/DR area.

C. FLAK SATELLITE INTERFACE

Chapter III dealt with VSATs in a general sense. This section will be devoted entirely to the specific solution that was chosen for implementation, research, and a technology demonstration to World Vision on April 26, 2005. Tachyon Networks Incorporated was the satellite provider that was used. The Tachyon network uses the Ku spectrum and is a Star topology with their corporate Gateway as the center. From the end user's CPE, the system uses Multi-frequency TDMA with a reservation based multiple access scheme. It uses broadcast Time Division Multiplexing (TDM) for multiple access from the Gateway back to the CPE (Tachyon, 2004). This system interfaces to the FLAK through an Ethernet connection.

1. Auto Deploy CPE

The Auto Deploy system is a compact solution that features automatic finding and alignment of the system's antenna to the satellite. It significantly reduces the expertise level required on site during setup by using a motorized system that automatically deploys the antenna, locates and locks on to the correct satellite, and sets up the Internet connection to Tachyon's network.

This system is a self contained VSAT solution that deploys in two separate cases for the ODU and the IDU. The dimensions and weight require two personnel for handling and deploying the ODU. Shipping concerns may arise when transporting the 260 pound, 53" X 19" X 43" case for this unit. However, those dimensions should be weighed against the ten minute deployment time as well as the connection speeds supported. The only assembly required is to connect the provided cables from the ODU to the IDU. Figure 21 shows the convenient storage of all needed cabling in the ODU cover.

Figure 21. Cable storage in ODU cover

Figure 22. Tachyon Auto Deploy ODU and IDU

Since the satellite is an additional requirement for connection, it is separate from the main FLAK components. However, the IDU can be readily integrated into the FLAK. The author's recommendation is to use the supplied seven rack unit case with Tachyon's Auto Deploy system to house the remaining equipment for the FLAK.

There are several key features that should be mentioned concerning the Auto Deploy system. The unit uses a .75 meter offset fed parabolic antenna which can limit areas for deployment and connection speeds. The supplied cabling supports power to the

ODU from the IDU up to 200 feet. The temperature requirements are most limited by the IDU which requires 0 to 40 degrees Celsius for the electronics. Power specifications support 110 – 125VAC and 50 – 60Hz input and draws 160 watts maximum power.

2. Fixed Access CPE

Price is always a factor in deciding a system solution. For that reason, a Fixed Access solution was tested as well. The difference in price between the Auto Deploy and the Fixed Access solutions was from $25,000 to $2,500 respectively. However, the decrease in price also means an increase in the assembly required and the expertise needed on site.

Additionally, the Fixed Access unit cannot be moved and transported in the same easy manner as the Auto Deploy system. The Fixed Access system is packaged, unassembled, in three large boxes. Once the system is unpacked, it is not easy to repackage for transporting.

The Fixed Access CPE requires several setup stages before being operational. These steps include antenna assembly, radio assembly, mount assembly, acquiring of the satellite and connection to the IDU. Setup of the system takes about three hours from start to finish for personnel conducting the task for the first time. Below is a list of installation requirements:

- Determine a suitable site for antenna
- Determine a suitable site for the IDU
- Assemble mount and antenna
- Assemble radio on antenna feed support
- Add ballast and tethering, if required
- Ground the system according to codes
- Set dish coarse azimuth
- Set transmit polarization and polarization offset
- Set dish elevation
- Point and peak the antenna
- Run a pair of IFL cables from the ODU to the IDU

- Connect a laptop/desktop PC to the IDU with a CAT5 crossover cable
- Power up the IDU and the PC
- Run the Tachyon Install Wizard on the PC
- Check for proper performance parameters
- Install line amplifier if needed

While the differences between the Auto Deploy and the Fixed Access systems are multiple, they offer similar WAN connections. The Fixed Access installation provided a 1.544 Mbps downlink and 512 Kbps uplink. A standard RJ45 Ethernet connection is then run to the FLAK.

D. FLAK ROUTER

The real work horse of the FLAK is the router. It enables flexibility by supporting a large number of WAN connections that might be available at any location. While the underlying concern is to have connectivity in remote locations (satellite), additional resources are planned to take advantage of wireless, T1/E1, Ethernet, ADSL, E&M, and FXO connections. After the WAN connection is established, the network administrator has the flexibility to set up multiple connected networks using NAT and VLANs.

The Cisco 2811 Integrated Services Router is chosen for the level of flexibility it offers, as well as additional applications it supports. The modular architecture and design allows this router to expand to support other needs of the network. The 2811 has two integrated 10/100 Mbps Ethernet ports, four high-speed WAN interface card (HWIC) slots and one Network Module Extended (NME) slot. There are over ninety different WAN interface cards, voice interface cards, and advanced integration modules. A recent test by Miercom Independent Testing Labs produced the following key findings:

- The new 2811 modular router concurrently runs IP-telephony, data, security, and other services.
- It can sustain two T1s with full bi-directional WAN data traffic, along with all services.
- Its modular hardware design allows highly tailored multi-service mix.

- It was tested with a fully integrated IP-PBX, voicemail, hardware-based IDS, firewall, NAT, and other services running (Miercom, 2004).

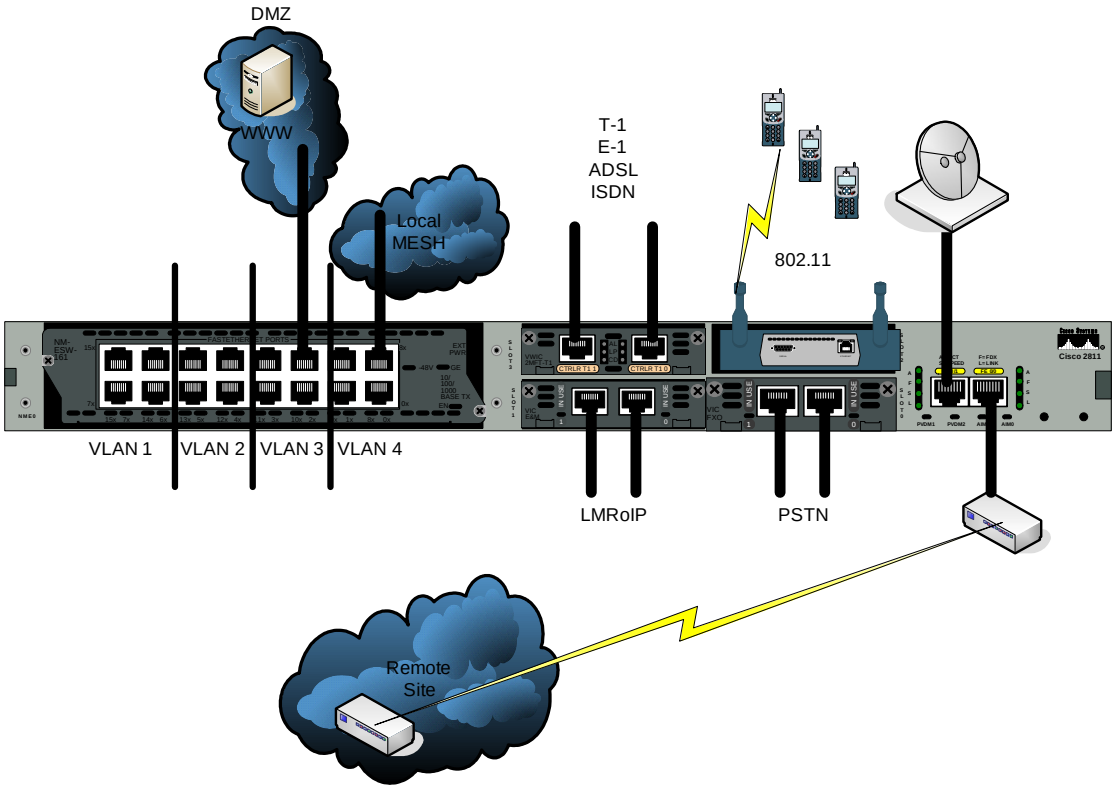


Figure 23. Router physical layout

1. Ethernet Ports

The router had two integrated 10/100 Ethernet ports. These ports were chosen to support connections that would be used the majority of the time and would leave the other resources open for flexibility. The satellite IDU for the Tachyon system, Redline 802.16 AN-50s, and most bridging equipment require a straight-through cable connection to the router's integrated Ethernet ports.

2. Wireless High-speed WAN Interface Card (HWIC)

A new addition to the available choices of modules for integrated service routers is the wireless HWICs. This is very convenient for the FLAK because it eliminates having an external wireless access point to support 802.11 users and wireless phones. The wireless HWIC is available in a form factor that supports 802.11a/b/g and provides

the same functionality as a traditional access point. While the planned implementation is to support local users and phones, the module can support fixed or external dipole or dual mode antennas. The following paragraphs will cover in detail other available features.

a. Security

Most standard security measures for 802.11 wireless are available for the wireless HWIC. Static Wired Equivalent Privacy (WEP) is supported up to 128 bits. Other security solutions available include versions of Extensible Authentication Protocol (EAP), EAP-Transport Layer Security (EAP-TLS), Pre-Shared Keys (PSK), Radius, and MAC filtering.

b. VLANs Over Wireless Network

VLANs are supported through the wireless HWIC. VLANs enable the system administrator to segment groups of users or devices into different broadcast domains, different multicast groups, and different security segments. This is the same concept that will be covered in greater detail later in the VLAN section.

c. Management

Several options for management are available. The wireless HWIC can be SNMP enabled and managed via a MIB browser. Additional management is available through any means to manage all other router interfaces which include:

- Command Line Interface (CLI)
- Telnet, SSH CLI
- HTTP browser interface
- Secure router and Device Manager (SDM) GUI

d. Other

Other features supported include Quality of Service (QoS) through traffic prioritization. All of the interfaces associated with the wireless HWIC can be configured as regular bridged or routed interfaces.

3. Foreign Exchange Office (FXO) Voice Interface Cards (VIC)

FXO VICs provide one way for the router to be an interface to the public switched telephone network (PSTN). The VIC 2FXO provides two ports that accept RJ-11 connectors and lines from the phone wall jacks, the Public Switched Telephone Network (PSTN) Central Office (CO) or a Private Branch eXchange (PBX). The FXO VIC does not provide dial tone to telephone sets and, while they will fit, phone cables should not be plugged into the FXO ports. The FXO VIC appears to the switch at the CO as a telephone. When using the VIC 2FXO module, the router can connect to two separate phone lines and support incoming and outgoing calls.

4. Ear and Mouth (E&M) VICs

The E&M VIC is used in the FLAK to support legacy types of equipment. Field units, emergency responders, and medical personnel are normally deployed with some type of radio solution. Command and Control (C2) of these units takes place at a headquarters that may be geographically separated by a large distance. Amplifiers, relay stations, and repeaters are used to maintain connection with deployed elements to the headquarters. E&M interfaces provide a connection where dispersed units can terminate their RF transmissions to be digitized and transmitted over an IP network. This technique is referred to as Land Mobile Radio (LMR) over IP (LMRoIP) (Cisco, 2005).

5. Remaining HWIC

The remaining HWIC slot for the router is available to support any available connections or specific missions of the FLAK. As a preliminary feature, additional modules are stored with the FLAK to support connections of opportunity. These are not limited to, but include:

- One WIC-1DSU-T1-V2, T1 RJ48 interface with built in DSU/CSU
- One HWIC-4ESW-POE, 4 port switch with power over Ethernet capability
- One WIC-1ADSL-I-DG, one port ADSL over ISDN

Other potential uses exist for this remaining HWIC slot. One attractive solution would be to use any two port interface cards and bond the lines to provide double the

bandwidth. This option was not implemented for the FLAK because it did not seem likely that two connections would be available at a disaster site. However, it is possible to use a T1 (2 port) multi-flex trunk WIC and aggregate the connections to provide effectively a three Mbps connection. This is done using a feature set offered by the Cisco Integrated Operating System (IOS) called Multiple Link Point to Point Protocol (MLPPP).

6. Network Module Extended (NME)

The NME is the last available slot on the router and can accept all NM and NME modules available. The NME provides flexibility and additional features which include caching solutions, intrusion detection systems (IDS), and others. For the FLAK the sixteen port PoE enabled Ethernet switch is used. Other available modules include:

- Intrusion Detection System network module
- Content Engines for performance and security
- Cisco Unity Express network module (supports voice mailboxes)
- Cisco Network Analysis module

VII. FLAK VIRTUAL LOCAL AREA NETWORKS (VLANS)

Computer networks are developed due to the desire to have multiple machines networked together at a location. Motivations include the need to share files, information, and so forth. Networked computers located in one geographic area are known as a LAN. As individuals construct their own LANs, the concept of a routed network is developed to allow communication between LANs. The local area network remains as a single broadcast domain of machines networked together. Up until the concept of VLANs, this has all done by physical connections.

VLANs create a logical means for physically separated devices to communicate as if they were on the same wire or network. When taken at face value, VLANs may not seem important. However, they afford a network administrator very flexible means of user management. The following are different types of VLANs:

A. PORT BASED VLAN

The port based or static VLANs deal mainly with a switch and the user's physical point of connection to that switch. Switch ports can be segmented and assigned to different VLANs. In this case clients across the switched network on corresponding VLAN segments appear to reside in the same LAN.

The port based option is what has been implemented currently on the FLAK. This approach is used because it offers organization, security, and management benefits. The integrated sixteen port switch is segmented into four different VLANs with four ports for each VLAN. VoIP phones can be limited to ports one through four with QOS enabled, while ports five through eight could be limited to only allow http traffic, and all local mesh clients could exist only on the network corresponding to ports nine through twelve on the switch. These are merely examples of what could be done.

B. MAC BASED VLAN

MAC filtering is a common means of providing security. Access lists similar to security uses can also be applied to users for VLAN assignment. MAC based VLANs are

an example of how users can dynamically be assigned to VLANs. This implementation uses a policy management server that associates users with the appropriate VLAN. Management of this type of assignment can be tedious for a large network where network interface cards (NICs) may fail. The MAC address of the replacement card has to be included for correct VLAN assignment.

C. PROTOCOL BASED VLAN

This type of VLAN is used to filter IP traffic.

D. ATM VLAN

This type of VLAN is used to provide a translation from an Ethernet network to an ATM network. This is more commonly referred to as LAN emulation (LANE) over ATM (Javvin, 2005).

E. ADVANTAGES OF VLANS:

- Broadcast control
- Security
- Performance
- Network management

VIII. FLAK VOICE OVER IP (VOIP) SERVICE

There are many different solutions for Voice over Internet Protocols (VoIP). Ondo is an open source PBX and Session Initiation Protocol (SIP) server. Asterisk is a Linux based PBX and SIP server. SIP is a peer-to-peer standard for multimedia conferencing over IP that uses a client/server architechture. End points can typically perform as User Agent Clients (UACs) or User Agent Servers (UASs) based on initiating a SIP request or responding to a request, respectively. End points can function as either a UAC or UAS per transaction.

A. ZYXEL PRESTIGE 2000W

ZyXEL manufactures several VoIP products. The Prestige 2000W is a wireless VoIP phone that supports SIP and can make calls directly between other SIP phones. This proved to be useful during the HFN in Thailand. When the network structure was at a minimum, any ZyXEL phones within WiFi coverage on the network could communicate together.

The only requirement per se is that the phones are configured as wireless clients for the network. The SSID, WEP, and all other pertinent data must be programmed into the ZyXEL phones. While it is possible to scan for available networks, security information, like the WEP key, has to be programmed in manually. This can be a frustrating task that requires entering a twenty-six digit hexadecimal key by phone number pad.

B. CISCO CALLMANAGER

Cisco CallManager is a software suite that is the center of Cisco's plan for Architecture for Voice, Video, and Integrated Data (AVVID). It normally runs on a Media Convergence Server (MCS), which is a proprietary server from Cisco. The CallManager provides a web browser environment to configure and manage IP phones, VoIP gateways, and other AVVID related equipment remotely. Search capabilities, default entries, and integrated help files are features provided by CallManager that assist

in administering devices. Several automated features simplify creating dial plans and call routes. The CallManager also provides advance enterprise services like call waiting, call forwarding, conferencing, music on hold, and other software features that can enhance capabilities (Cisco Systems, Inc., 2001). Compatibility information for Cisco CallManager can be acessed at http://www.cisco.com/univercd/cc/td/doc/product/voic/c_callmg/ccmcomp.htm.

Primary functions performed by the CallManager include:

- Call processing
- Signaling and device control
- Dial plan administration
- Phone feature administration
- Directory services
- Operations, Administration, Maintenance, and Provisioning (OAM&P)
- Programming interface to devices and applications

Cisco IP telephone deployment models include: single site, multi-site WAN with central processing, multi-site WAN with distributed call processing, clustering over the IP WAN. The single site deployment model was researched for the FLAK. Current implementation, however, uses the CallManager Express to limit hardware devices.

A single site deployment model is a typical solution for small network requiring voice support. This site consists of one CallManager or CallManager Express on the network that processes all VoIP calls. Rapid deployment of a HFN may be employed and supported with the single site model for local calls over the network. Phone calls made beyond the network must be supported by the PSTN. However, there is not a limitation on where PSTN calls terminate. For example, a VoIP call can be initiated from the LAN, use the PSTN to carry the voice traffic, and terminate at another single site deployment.

This model is beneficial for local communication. While this may be important, to take advantage of the available cost savings for making phone calls over the WAN calls must be configured in the dial plan to other voice gateways. All calls made over the PSTN will be charged as normal calls originating from the existing local phone.

C. CALLMANAGER EXPRESS (CME)

CME is a slimmed down version of the CallManager solution that is integrated into the IOS of a voice gateway router. This allows a considerable cutback on hardware required for the FLAK, but maintains the needed functionality to support VoIP calling. CME has limitations and can only support up to thirty-six phones on the current FLAK design. Documentation for current CME installation, management, and specifications can be found at http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/itscdc/itsph.htm.

THIS PAGE INTENTIONALLY LEFT BLANK

IX. FLAK INTEGRATION WITH WIRELESS LOCAL MESH NETWORKS

A. OVERVIEW

Extending services to users on a LAN is a primary requirement for the FLAK. The most desirable way accomplish this is through wireless clients. Additionally, adding a mesh capability allows each client to independently route traffic to other users. This benefits traffic loads, flexibility, and redundancy.

Developing the FLAK, the author chose two mesh solutions to perform a high level but relatively thorough examination of mesh nodes. This was done using clients with 802.11b Ad-Hoc with OLSR and the WMC6300 Motorola/ITT MeshNetworks Enabled Architecture (MEA) card (TNT 05-2, 2005). Results from this test give an idea of the connected user capabilities.

B. 802.11B

The 802.11b standard is part of the 802.11 wireless families of standards that began as early as 1989 and were intended to provide a wireless equivalent to Ethernet. 802.11b was the first wireless LAN standard to be defined and commercially adopted by equipment manufacturers. Initially, the standard was designed to provide about a 300 meter distance between devices and support general data traffic. However, advances have made it possible to accommodate forms of streaming data like audio and video as well as distances up to 50 miles with the appropriate equipment.

802.11b uses a direct sequence spread spectrum technology with eleven defined channels that are in the 2.4 GHz band and are 22 MHz wide. Most commonly, three channels -- one, six, and eleven -- are used because they offer the least amount of frequency overlap. The advertised or theoretical maximum data rate is 11 Mbps but actual rates are closer to 5 Mbps. 802.11b provided the layer one and layer two (Ad-Hoc) representations for the Wifi Mesh nodes.

Similar standards (802.11 a, 802.11g), and others exist that can be used in place of 802.11b. These implementations have the potential to perform differently, but were not considered for this test.

C. OLSR

Optimized Link State Routing Protocol (OLSR) is a proactive routing protocol for Mobile Ad hoc NETworks (MANET). The protocol uses a link state algorithm. OLSR is an optimization over the classical link state protocol, tailored for mobile ad hoc networks. It is designed to work in a completely distributed manner and does not depend on any central entity. All nodes send periodic hello messages and mitigate to propagate route tables.

OLSR is one of several MANET protocols. It operates as a table driven, proactive protocol, i.e., exchanges topology information with other nodes of the network regularly. Each node selects a set of its neighbor nodes as Multi-Point Relays' (MPR). In OLSR, only nodes, selected as such MPRs, are responsible for forwarding control traffic, intended for diffusion into the entire network. MPRs provide an efficient mechanism for flooding control traffic by reducing the number of transmissions required.

D. ITT MESHNETWORKS ENABLED ARCHITECTURE (MEA)

This is a proprietary solution offered by Motorola. MEA technology supports both infrastructure and client meshing. MEA’s client meshing enables end users to instantly form a broadband wireless network among each other – with or without the inclusion of network infrastructure. As users join the network, network coverage and throughput can increase, providing alternative routes for traffic. MEA networking is unique in that it supports Continuous Mesh routing. That is, it supports simultaneous operation of infrastructure and client meshing while allowing clients to move seamlessly between infrastructure-based and client-based peer-to-peer networks (MEA, 2003). This experiment only implemented the subscriber device with the WMC6300 wireless card.

Motorola's MeshNetworks Enabled Architecture (MEA) technology leverages proven Ad-hoc On-demand Distance Vector (AODV) routing techniques originally

developed for battlefield communications (Reimer et al., 2005). Because this is a proprietary solution, there are disadvantages, but the MEA technology provides some unique improvements over 802.11b and mesh solutions built on that technology. The following paragraphs give an overall idea of high level implementation.

> Self-forming, self-healing routing intelligence distributes clients among Access Points, eliminating bottlenecks and improving overall network performance. MEA technology also improves network robustness, as clients can hop to alternate Access Points if their current Access Point is congested or fails. Clients can form large, ad hoc peer-to-peer networks virtually anywhere, anytime. Peer-to-peer networking reduces the demand on network Access Points, freeing up capacity for other users. All these capabilities create low-cost, seamless and simple to deploy wireless PAN, LAN or WAN solutions (MEA, 2003).

Parameter	Description
Frequency Range	2.400 – 2.480 GHz, 4 channels
Power Output	+23 dBm minimum
Receive Sensitivity	-90 dBm
Operating Temperature Range	-35 degrees Celsius to +55 degrees Celsius
Data Rates (burst)	1.5 Mbps, 3.0 Mbps, 4.0 Mbps, 6.0 Mbps
Modulation	QPSK/BPSK
Antenna Gain	
Infrastructure Devices	4 and 8 dBi
Mobile Devices	0 and 3 dBi
Subscriber Devices	2 dBi

Table 3. MEA Hardware Performance Summary (From MEA, 2003)

MEA equipment differs from 802.11 wireless in many key hardware performance characteristics. Similar to WiFi, MEA uses an 80 MHz range, 2.4 GHz – 2.48GHz for communication. A four channel implementation is used where one reserved channel

negotiates conversations and three channels are then used for station conversations. Radio processors use a rake receiver which provides better resilience to multi-path interference. The rake receiver technique uses several baseband correlators to individually process several signal multi-path components. The correlator out-puts are combined to achieve improved communications reliability and performance. In other words, additive signal components are combined to provide improved signal quality. Additional differences include the following features:

- Forward Error Correction (FEC)
- Adaptive Transmission Protocol (ATP): This protocol intelligently adjusts transmit power and transmission speed to improve communication links. A common situation of the Near / Far Node problem is solved through this enhancement
- Multi-hopping Capability
- Increased Mobility Support

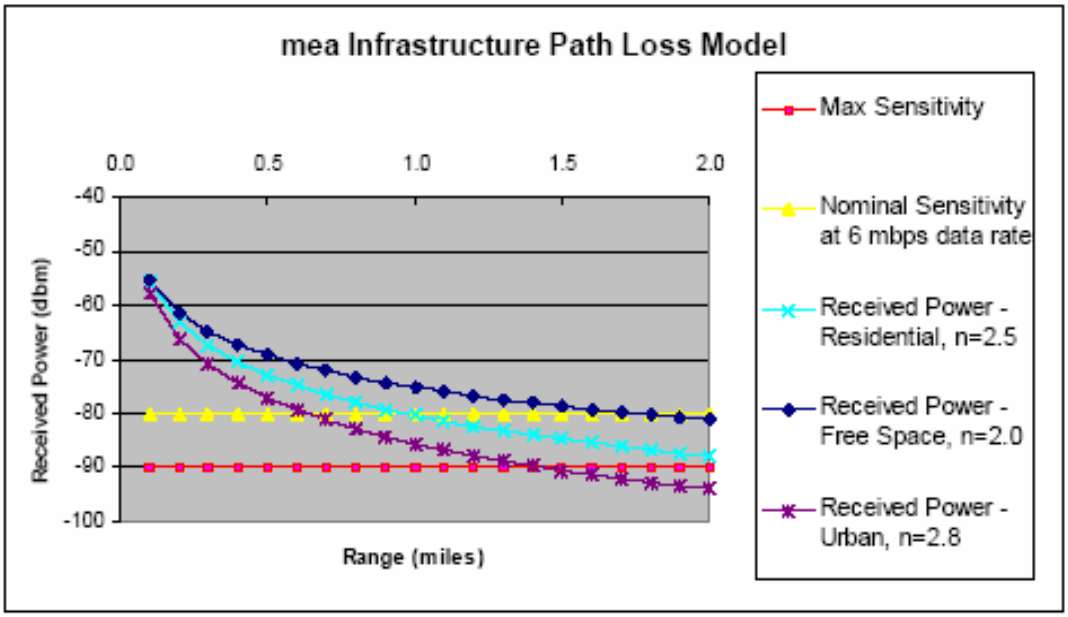


Figure 24. Advertised Path Loss (From MEA, 2003)

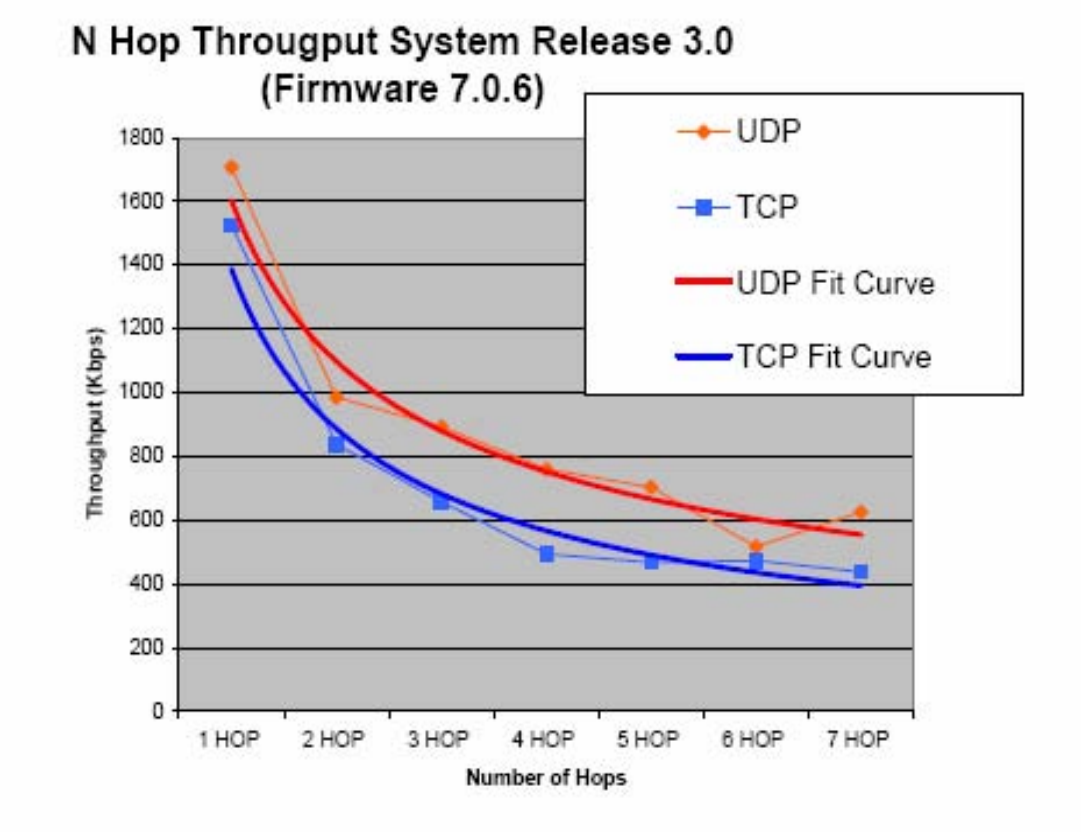
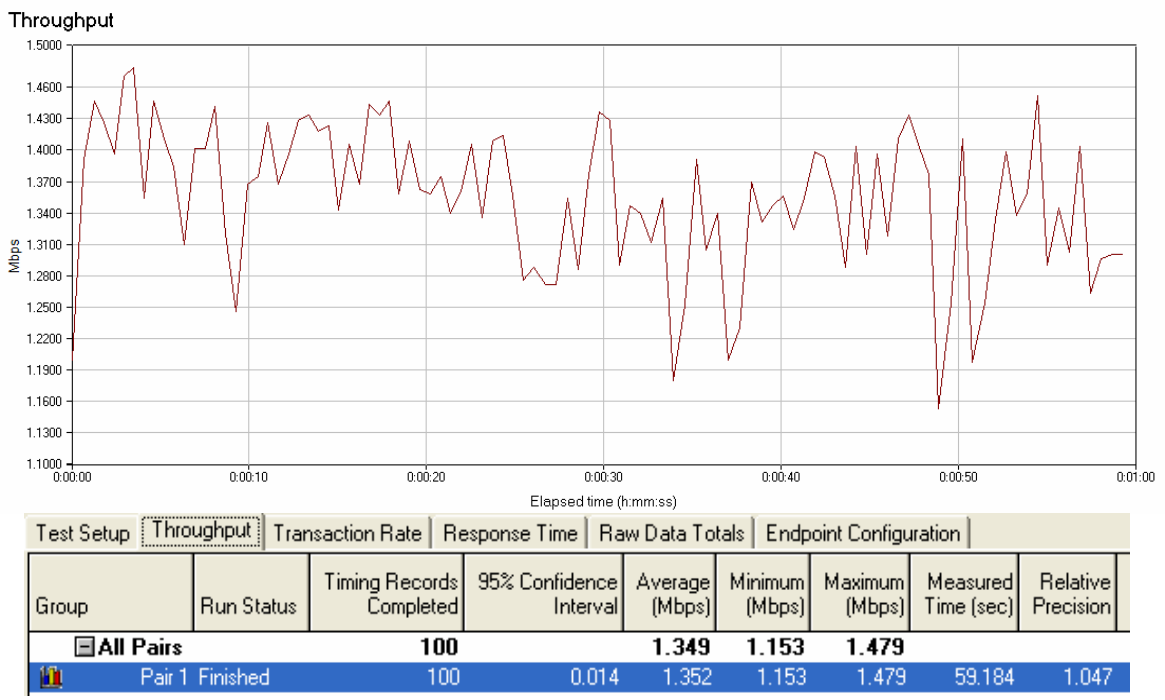


Figure 25. Advertised Throughput Per Hop (From MEA, 2003)

This technology has been tested using the Redline AN50 as a means to extend last-mile wireless service. Some other typical methods have been to use T1, DSL, Cable, or Fiber. The native interface for the IAPs is Ethernet and allows for COTS WAN bridging technology.

Quick tests were conducted to verify the support of IxChariot endpoints and scripts. This test was conducted without any difficulties and presented the following characteristics for basic throughput testing:



Test Setup | Throughput | Transaction Rate | Response Time | Raw Data Totals | Endpoint Configuration

Group	Run Status	Timing Records Completed	95% Confidence Interval	Average (Mbps)	Minimum (Mbps)	Maximum (Mbps)	Measured Time (sec)	Relative Precision
All Pairs		**100**		**1.349**	**1.153**	**1.479**		
Pair 1	Finished	100	0.014	1.352	1.153	1.479	59.184	1.047

Figure 26. IxChariot Gut Check

E. TEST SETUP

The general test setup involved creating MANETs with rugged PDA's called Tacticomps from Inter-4 (Inter-4, 2005). The first run through used the 802.11b WiFi cards. A specific and tedious order of tasks had to be performed to obtain a working WiFi MANET. The following list documents those tasks:

- Setup clients with SSID for an AD-HOC network
- Confirm inter-client communication and formation of the AD-HOC network
- Run the OLSR routing program on each Tacticomp
- Ensure that routes are populated to all clients
- Deploy clients to positions noted in Figure 27

This process was tedious and error prone

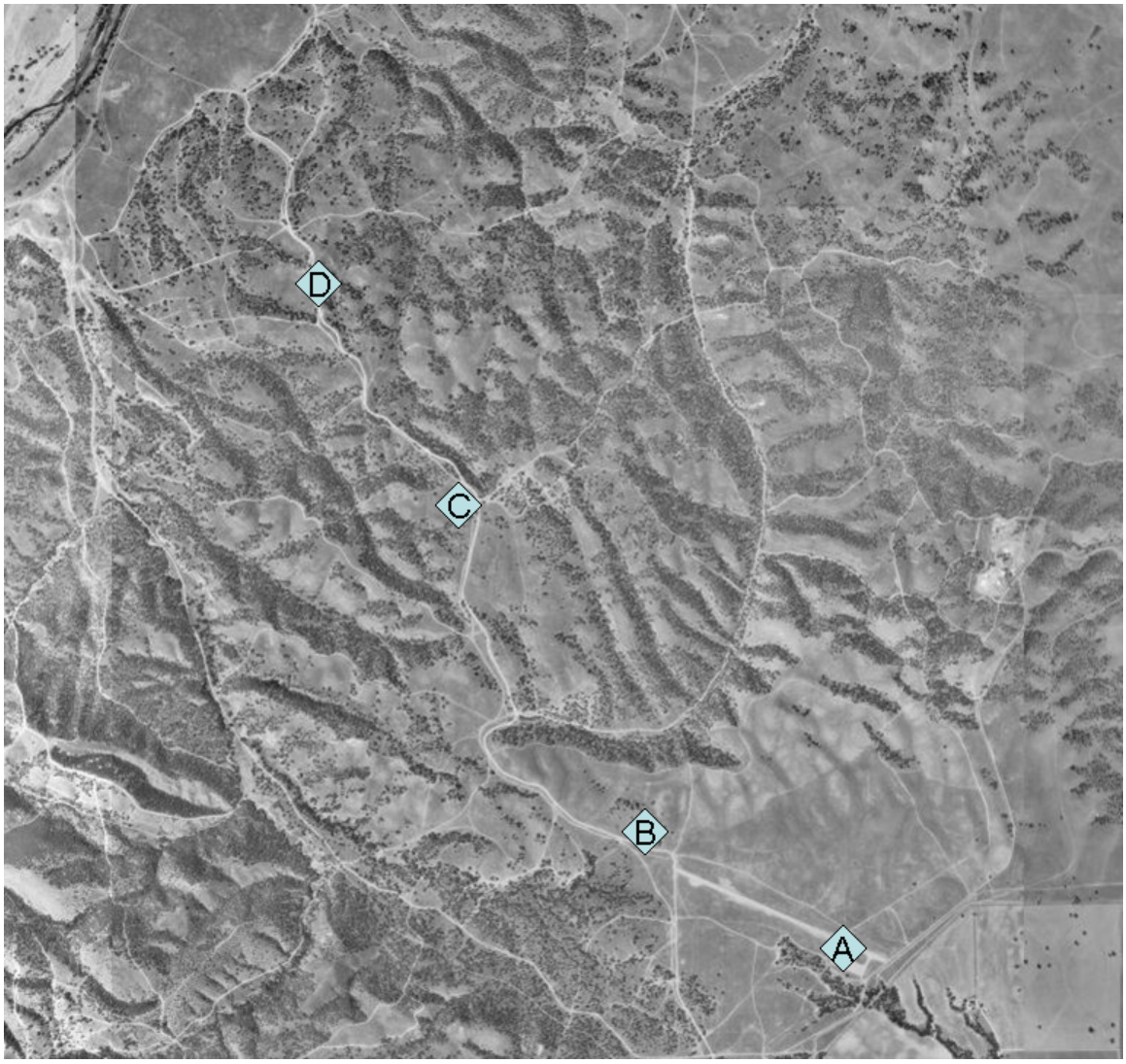


Figure 27. Camp Roberts Test Setup

The node layout was as follows: Node A was located at the TOC, Node A to B was 1.4 kilometers, Node B to C was 2.1 kilometers, Node C to D was 1.3 kilometers. The tests were run in an exhaustive manner to test the all possible node combinations for source and destination. This gave a good understanding of the overall characteristics and provided a maximum link of 4.8 kilometers with three hops. Results are presented by source node and show the characteristic of the throughput as the distance for the overall link increased.

The second run through used the Tacticomps with WMC6300 MEA cards. Network setup was complete in about ten minutes. The process for establishing the MANET was to merely turn on the clients. Routes automatically populated and where

easily monitored on the MeshView software provided. The MEA cards definitely out performed the WiFi implementation regarding ease of setup.

The script that was used to conduct the measurements was a basic file send script. Figure 28 shows the actual script constructed in the IxChariot script editor. Notice how portions of the script are separated according to the respective endpoint. This script simulated sending a 10 kilobyte file one hundred times. Compression was not used. The default for the buffer size and the maximum data rate for sending were both used. This was an appropriate measurement that provided throughput averages with "T-values" of about 0.03 for a 95% confidence interval.

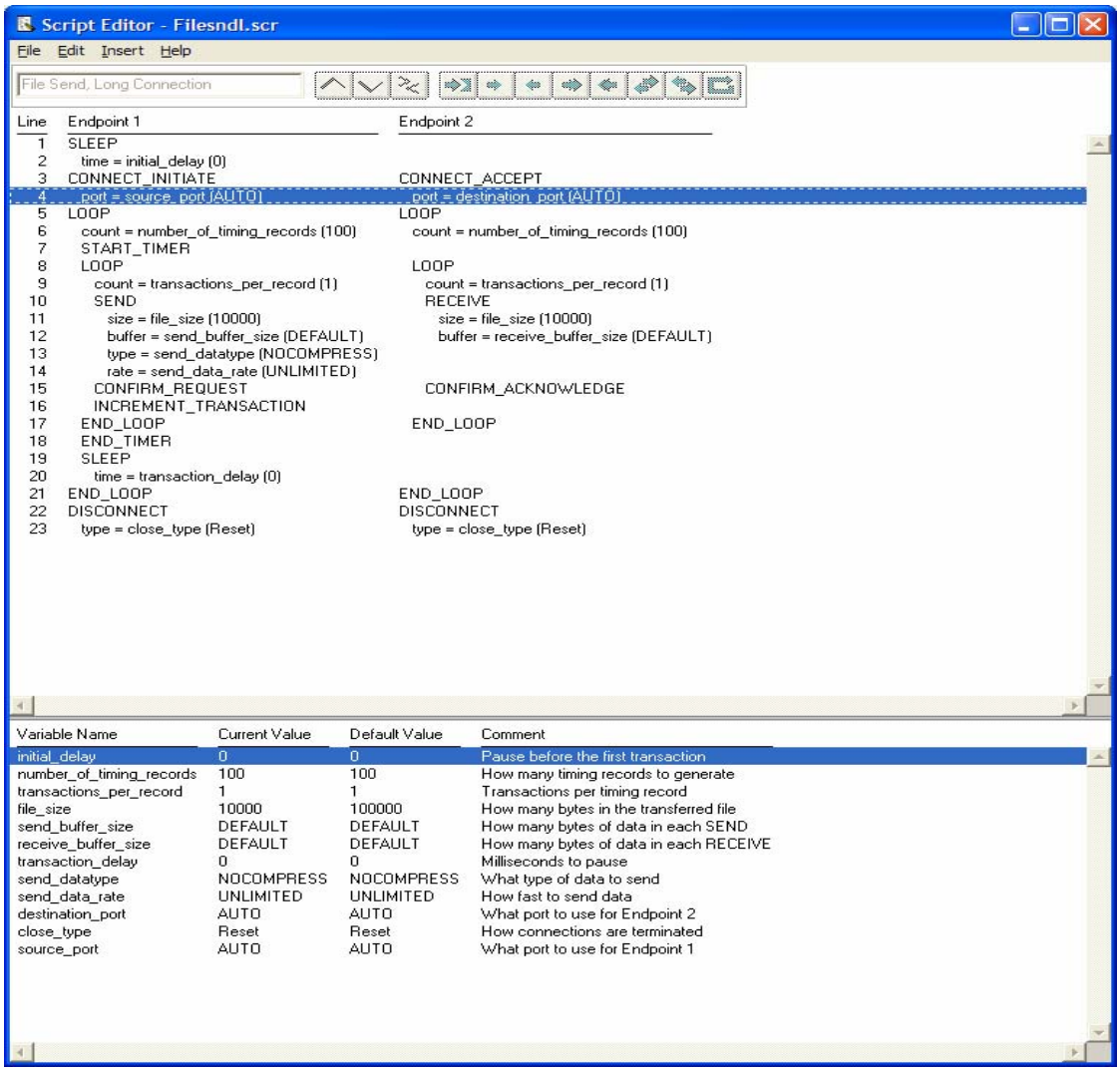


Figure 28. Test Script

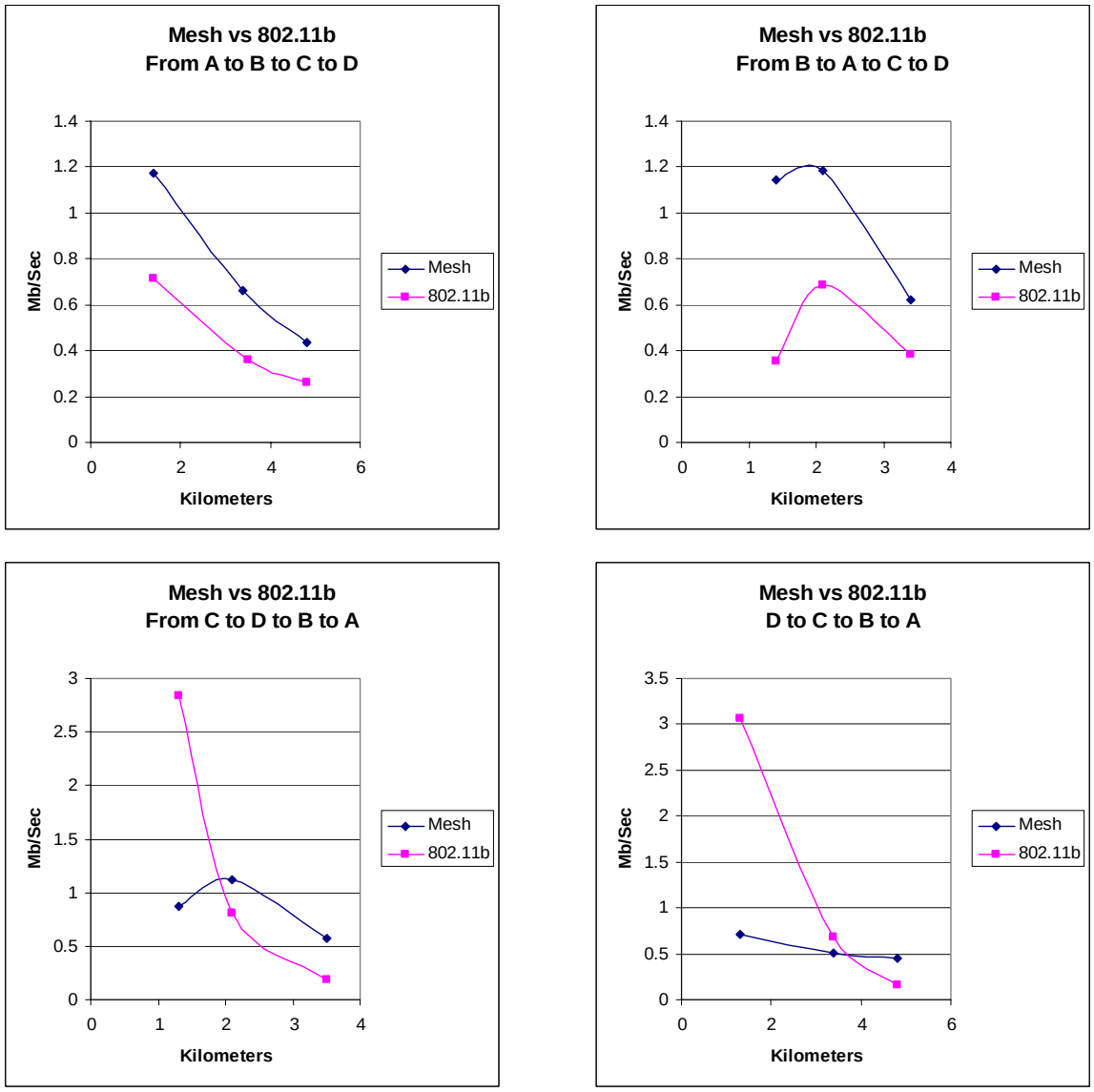


Figure 29. Test Results

The test results verify expected characteristics concerning the throughput in two areas: number of hops and distance. As the number of hops increase, the throughput decreases. These results are supportive of the hop characteristics from Figure 25. Also, an increase in distance causes a decrease in throughput.

The two lower charts from Figure 29 show interesting characteristics of the RF environment. Wireless networking is generally conducted in an unlicensed band. This increases the chance that other people are using their devices and causing undesired

competition for the air waves. Nodes D and C are isolated from other wireless devices and have a much greater throughput capability between each other. In all other cases, the co-channel interference from other wireless devices at located in the vicinity of node A cause a degradation of service.

X. CONCLUSION AND FOLLOW ON RESEARCH

A. CONCLUSION

Designing a FLAK to support HFNs for HA/DR is an interesting but broad subject. Many topics from within this thesis provide areas for additional research. Some areas are technical, but others deal with people and processes. The tsunami of December 26, 2004 provided opportunities to observe how both the technology and the people performed and in many cases did not perform.

General requirements that the FLAK must support include connection to the Internet through some reach-back means, the ability to support last-mile connections, and the ability to support a flexible LAN. One of the greatest challenges is to operate the FLAK in a primitive or isolated environment and possibly with limited access to technical support.

B. CIVIL-MILITARY COMMUNICATIONS

Additional research in the area of civil-military communications is needed. In the author's opinion, this area will begin to improve once the Global Information Grid becomes more of a reality. The technology aspects are challenging, but the greatest impact can be made in the area of processes and people.

C. SATELLITE CONNECTIONS

Solutions for improving IP over satellite connections are being developed today. Some solutions include being implemented by service providers, such as Tachyon. Other solutions are hardware devices performing caching, protocol enhancements, and software implementations. Further research should address additional ways to mitigate problems for IP over satellites and test solutions that are being provided.

D. MESH ENABLED ARCHITECHTURE (MEA)

MEA and MANETs in general require additional research. Field experiment programs at the Naval Postgraduate School are providing good opportunities for this type

of work to continue. An important area that needs additional research is how this type of network bridges to other terrestrial or traditional types of networks. The current proprietary nature of these products limits their use in the FLAK.

LIST OF REFERENCES

Allman, M. (1999, January). RFC 2488, *Enhancing TCP over satellite channels using standard mechanisms.* Retrieved May 31, 2005, from http://www.faqs.org/rfcs/rfc2488.html

Barge, Hezekiah, Jr.; Davis, Mark S.; Schwent Jr., John T. *Field Level Information Colloaboration During Complex Humanitarian Emergencies and Peace Operations.* Master Thesis. Naval Postgraduate School. June 2003

Brewin, Bob. (2005, Apr 25). *Operation Tsunami Aid by Bob Brewin.* Retrieved May 5, 2005 from http://www.fcw.com/article88654-04-05-Print

Buddenberg, Rex. *Information Security.* Retrieved June 10, 2005 from http://web1.nps.navy.mil/%7Ebudden/lecture.notes/infosec/infosec_notes.html

Carr, Joseph J. (2001). *Practical antenna handbook* (4th ed.). New York: McGraw-Hill

Center of Excellence in Disaster Management and Humanitarian Assistance. (2005). Indian Ocean Earthquake Tsunami Emergency Report, dated December 31, 2004. Retrieved May 16, 2005, from COE-DMHA Web site: http://coe-dmha.org/tsunami.htm Citation: Center of Excellence in Disaster Management and Humanitarian Assistance [COE-DMHA], 2005)

Cisco Systems, Inc. (2001). *Cisco CallManager Administration Guide*. Retrieved May 26, 2005, from http://www.cisco.com/

Cisco Systems, Inc. (2005, February 3). *Cisco land mobile radio over IP solution reference network design*. Retrieved May 27, 2005, from http://www.cisco.com

Ford, Todd D.; Hogan, James L.; Perry, Michael W. *Comunication During ComplexHmanitarian Emergencies: Using Technology to Bridge the Gap.* Master Thesis. Naval Postgraduate School. September 2002

Garcia and Joseforsky. (2004, June).*Transformational communications architecture for the unit operations center (UOC); common aviation command and control system (CAC2S); and command and control* on-*the-move network, digital over-the-horizon relay (CONDOR).* Master Thesis. Naval Postgraduate School

Headquarters, Department of the Army. (2000). *The Army satellite communications architecture book. Fort Gordon: TRADOC*

Inter-Agency Standing Committee Working Group. (2004, June). *Civil-military relationships in complex emergencies.* June 28, 2004 from http://ochaonline.un.org/mcdu/guidelines

Javvin Company. (2005, June). Protocol Dictionary. *VLAN: virtual local area network and IEEE 802.1Q*. Retrieve June 3, 2005, from http://www.javvin.com/protocol/VLAN.html

Krulak, C.C. (1999, January). *The strategic corporal: Leadership in the three block war*. Retrieved May 5, 2005, from http://www.au.af.mil/au/awc/awcgate/usmc/strategic_corporal.htm

Mesh Networks, Inc,. (2003). *MeshNetworks guidelines for network deployment.* pp 1-6

Miercom lab testing summary report. (2004, September). *Cisco 2811 integrated services router*. p. 1. Retrieved June 2, 2005, from http://www.cisco.com/application/pdf/en/us/guest/ products/ps5854/prod_white_papers_list.html

Monti, Medio (Col, USMC). (2005, May). *Unified Assistance Combined Support Force-536, a Team of Teams.* Indian Ocean Tsunami Disaster Relief Workshop, Chiang Mai, Thailand

Office of Force Transformation. (2005, January 5). *The Implementation of Network-Centric Warfare.* Washington, D.C., U.S. Government Printing Office

Raimer, Glenn; Wentworth, John; Whitehill, Eric. (2005, February). Interview

Tachyon Networks. (2004). *How information was meant to travel; Technology overview*

Tactical Network Topology 05-2 Report. (2005, February). Naval Postgraduate School

United States Department of Defense. (2003, April 10) *Transformation Planning Guidance.* Retrieved May 02, 2005, from The Office of Force Transformation Web Site: http://www.oft.osd.mil/library/library.cfm?libcol=6

World Vision. (2005, April 26). Demonstration to World Vision at Fort Ord

World Wide Consortium for the Grid. (2005). Retrieved May 26, 2005, from http://www.w2cog.org

http://www.knoppix.net (2005, June)

http://www.dataline.com (2005, June)

http://inter-4.com (2005, June)

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDE, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. Alex Bordetsky
   Naval Postgraduate School
   Monterey, California

8. Brian Steckler
   Naval Postgraduate School
   Monterey, California

9. Rex Buddenberg
   Naval Postgraduate School
   Monterey, California

10. Brian Fila
    OSD, NII

11. Dan Boger
    Naval Postgraduate School
    Monterey, California